Original Article Open Access

The Iranian Association of Medical Law

Medical Law Journal

2026; 20: e53

Journal Homepage: http://ijmedicallaw.ir

Institute of Bioethics and Health Law

Criminal Liability Arising from the Possession of Sensitive Medical Data: Assessing the Grounds for Criminalization and the Challenges of Digital Health Criminal Policy

Zohreh Nikfarjam[1*], Sayed Mohammad Keykavosi[2]

1. Department of Jurisprudence and Principles of Law, YI.C., Islamic Azad University, Tehran, Iran.
2. Department of Jurisprudence and Fundamentals of Islamic Law, Member of the Young Researchers Club, YI.C., Islamic Azad University, Tehran, Iran.

ABSTRACT

Background and Aim: With the expansion of digital health infrastructure and the increasing reliance of healthcare systems on electronic health records, sensitive medical data have become a vital component of information governance. In this context, changes in data architecture and the expansion of access to and storage of medical information have turned the issue of the unauthorized possession of medical data into a significant challenge for contemporary criminal policy. This challenge is associated, on the one hand, with patients' fundamental rights, privacy, and informational dignity and, on the other, with the cybersecurity of healthcare infrastructure. This study aims to examine the legal grounds and conditions for criminalizing the unauthorized possession of sensitive medical data and to assess whether such an approach could be adopted within the Iranian legal system.

Method: This study employs a descriptive-analytical method with a comparative approach. Research data were collected through the examination of documentary and library-based sources, relevant laws and regulations, judicial decisions, and legal scholarship from selected countries. These materials were analysed using legal and comparative methods. In this process, the grounds for criminalizing the unauthorized retention and possession of medical data were assessed with particular emphasis on the principles of legality of crimes and punishments, the harm principle, proportionality, and the requirements of privacy and information security protection.

Ethical Considerations: This study has observed the principles of academic integrity, accurate referencing, avoidance of distortion or biased selection of data, and respect for the rights of authors of scholarly works.

Results: The findings indicate that, in certain leading legal systems, the criminal-law approach to medical data is evolving beyond an exclusive focus on the actual disclosure of data towards the recognition and regulation of the potential risks arising from their unauthorized retention. Accordingly, the possession of sensitive medical data may constitute a criminal offence where it occurs without legal authorization or in breach of security requirements and is capable of creating a significant risk to privacy, information security, or trust in healthcare relationships. However, the findings also indicate that criminalizing the mere state of possessing data, without establishing conditions such as lack of authorization, attribution of the conduct to the accused, and the existence of a significant risk, is incompatible with fundamental principles of criminal law, particularly the principles of legality, harm, and proportionality. Accordingly, distinguishing between legitimate professional storage of medical data and unauthorized, risk-generating retention is an essential condition for the legitimacy of criminal-law intervention.

Conclusion: Criminalizing the unauthorized possession of sensitive medical data may be justified within the framework of preventive criminal policy, with the aim of protecting privacy and the security of health data, provided that its scope is precisely and narrowly defined. Accordingly, it is recommended that the Iranian legal system clearly define the concepts of "sensitive medical data," "possession," and "unauthorized retention," distinguish legitimate professional handling of such data from risk-generating forms of unauthorized retention, and establish a balanced model of criminalization in accordance with the principles of legality, necessity, and proportionality. Such a model should, on the one hand, prevent excessive expansion of criminal law and overcriminalization and, on the other, ensure effective protection of health data.

Keywords: Digital Health; Sensitive Medical Data; Criminal Liability; Criminalization

Corresponding Author: Zohreh Nikfarjam; **Email:** znikfarjam@iau.ac.ir

Received: April 29, 2026; **Accepted:** August 04, 2026; **Published Online:** October 15, 2026

Please cite this article as:

Nikfarjam Z, Keykavosi SM. Criminal Liability Arising from the Possession of Sensitive Medical Data: Assessing the Grounds for Criminalization and the Challenges of Digital Health Criminal Policy. Medical Law Journal. 2026; 20: e53.

Copyright©2026, the Authors. This open-access article is published under the terms of the Creative Commons Attribution 4.0 International License which permits Share (copy and redistribute the material in any medium or format for any purpose, even commercially) and Adapt (remix, transform and build upon the material for any purpose, even commercially) under CC BY 4.0 terms.

دسترسی آزاد | مقاله پژوهشی

مجله حقوق پزشکی

دوره بیستم، ۱۴۰۵

Journal Homepage: http://ijmedicallaw.ir

مسئولیت کیفری ناشی از داشتن داده‌های پزشکی حساس:

ارزیابی مبانی جرم‌انگاری و چالش‌های سیاست کیفری سلامت دیجیتال

زهره نیک‌فرجام[1]*، سیدمحمد کیکاوسی[2]

۱. گروه فقه و مبانی حقوق اسلامی، واحد یادگار امام خمینی (ره) شهر ری، دانشگاه آزاد اسلامی، تهران، ایران.

۲. گروه فقه و مبانی حقوق اسلامی و عضو باشگاه پژوهشگران جوان، واحد یادگار امام خمینی (ره) شهر ری، دانشگاه آزاد اسلامی، تهران، ایران.

چکیده

زمینه و هدف: با گسترش زیرساخت‌های سلامت دیجیتال و افزایش وابستگی نظام‌های درمانی به پرونده‌های الکترونیک سلامت، داده‌های پزشکی حساس به یکی از عناصر حیاتی حکمرانی اطلاعات تبدیل شده‌اند. در این میان، تحول در معماری داده و گسترش دسترسی و ذخیره‌سازی اطلاعات پزشکی، مسأله «داشتن (Possession)» داده‌های پزشکی بدون مجوز قانونی را به چالشی مهم در سیاست کیفری معاصر تبدیل کرده است؛ چالشی که از یک‌سو با حقوق بنیادین بیماران، حریم خصوصی و کرامت داده‌ای آنان و از سوی دیگر با امنیت سایبری زیرساخت‌های سلامت ارتباط دارد. پژوهش حاضر با هدف بررسی مبانی و شرایط جرم‌انگاری داشتن غیر مجاز داده‌های پزشکی حساس و ارزیابی امکان پذیرش این رویکرد در نظام حقوقی ایران انجام شده است.

روش: این پژوهش با روش توصیفی ـ تحلیلی و رویکرد تطبیقی انجام شده است. داده‌های پژوهش از طریق مطالعه اسناد و منابع کتابخانه‌ای، قوانین و مقررات مرتبط، آرای قضایی و ادبیات حقوقی کشورهای منتخب گردآوری و با استفاده از روش تحلیل حقوقی و تطبیقی بررسی شده‌اند. در این فرایند، مبانی جرم‌انگاری نگهداری و داشتن غیر مجاز داده‌های پزشکی با تأکید بر اصول قانونی‌بودن جرم و مجازات، اصل ضرر، اصل تناسب و الزامات حمایت از حریم خصوصی و امنیت اطلاعات ارزیابی شده است.

ملاحظات اخلاقی: در این پژوهش، اصول امانتداری علمی، استناد دقیق به منابع، پرهیز از تحریف یا گزینش جهت‌دار داده‌ها و رعایت حقوق پدیدآورندگان آثار علمی مورد توجه قرار گرفته است.

یافته‌ها: یافته‌های پژوهش نشان می‌دهد که در برخی نظام‌های حقوقی پیشرو، رویکرد کیفری نسبت به داده‌های پزشکی از تمرکز صرف بر «افشای بالفعل داده» به سمت شناسایی و کنترل «خطر بالقوه ناشی از نگهداری غیر مجاز داده» در حال تحول است. بر این اساس، داشتن داده‌های پزشکی حساس، در صورتی که بدون مجوز قانونی یا برخلاف الزامات امنیتی صورت گیرد و قابلیت ایجاد خطر معنادار برای حریم خصوصی، امنیت اطلاعات یا اعتماد درمانی را داشته باشد، می‌تواند واجد وصف کیفری شود. با این حال، یافته‌ها نشان می‌دهد که جرم‌انگاری صرفِ وضعیت داشتن داده، بدون احراز شرایطی همچون غیر مجازبودن، قابلیت انتساب و وجود خطر معنادار، با اصول بنیادین حقوق کیفری، به ویژه اصل قانونی‌بودن، اصل ضرر و اصل تناسب، سازگار نیست. از این رو، تفکیک میان نگهداری حرفه‌ای و مشروع داده‌های پزشکی و نگهداری غیر مجاز و خطرزای آن، شرط اساسی مشروعیت مداخله کیفری است.

نتیجه‌گیری: جرم‌انگاری داشتن غیر مجاز داده‌های پزشکی حساس می‌تواند در چارچوب سیاست جنایی پیشگیرانه و با هدف حمایت از حریم خصوصی و امنیت داده‌های سلامت قابل توجیه باشد؛ مشروط بر آنکه قلمرو آن به صورت دقیق و محدود تعریف شود. بر این اساس، پیشنهاد می‌شود نظام حقوقی ایران ضمن تعریف روشن مفاهیم «داده پزشکی حساس»، «داشتن» و «نگهداری غیر مجاز»، میان تصرف مشروع و حرفه‌ای در داده‌ها و وضعیت‌های خطرزای ناشی از نگهداری غیر مجاز تمایز قائل شود و با رعایت اصول قانونی‌بودن، ضرورت و تناسب، الگوی متوازنی برای جرم‌انگاری این رفتار طراحی کند؛ الگویی که از یک‌سو مانع تورم کیفری و جرم‌انگاری افراطی و از سوی دیگر تضمین‌کننده حمایت مؤثر از داده‌های سلامت باشد.

واژگان کلیدی: سلامت دیجیتال؛ داده‌های حساس پزشکی؛ مسئولیت کیفری؛ جرم‌انگاری

نویسنده مسئول: زهره نیک‌فرجام؛ **پست الکترونیک:** znikfarjam@iau.ac.ir

تاریخ دریافت: ۱۴۰۵/۰۲/۰۹؛ **تاریخ پذیرش:** ۱۴۰۵/۰۵/۱۳؛ **تاریخ انتشار:** ۱۴۰۵/۰۷/۲۳

خواهشمند است این مقاله به روش زیر مورد استناد قرار گیرد:

Nikfarjam Z, Keykavosi SM. Criminal Liability Arising from the Possession of Sensitive Medical Data: Assessing the Grounds for Criminalization and the Challenges of Digital Health Criminal Policy. Medical Law Journal. 2026; 20: e53.

تمامی حقوق انتشار این اثر، متعلق به پژوهشکده اخلاق زیستی و حقوق سلامت پارس می‌باشد.

مقدمه

داده‌های پزشکی در عصر حکمرانی دیجیتال، مهم‌ترین و حساس‌ترین طبقه داده‌های شخصی محسوب می‌شوند، زیرا حاوی اطلاعاتی درباره وضعیت جسمی، روانی، ژنتیکی و زیستی افراد هستند که افشا یا سوءاستفاده از آن‌ها می‌تواند پیامدهای گسترده‌ای همچون تبعیض شغلی، آسیب‌های روانی، برچسب‌گذاری اجتماعی و نقض کرامت انسانی به همراه داشته باشد (۱).

در دهه اخیر، گسترش پرونده‌های الکترونیک سلامت، سیستم‌های هوشمند تشخیص پزشکی، ذخیره‌سازی ابری داده‌های درمانی و فناوری‌های پوشیدنی سلامت، موجب شده است که حجم بی‌سابقه‌ای از داده‌های حساس توسط نهادهای درمانی، شرکت‌های فناوری و حتی اپلیکیشن‌های تلفن همراه نگهداری شود. این تحول باعث شده است مسأله «نگهداری و داشتن داده‌های پزشکی» به یکی از مهم‌ترین محورهای سیاست‌گذاری کیفری و امنیتی تبدیل شود (۲).

آنچه امروز توجه حقوقدانان و نهادهای تنظیم‌گر را به خود جلب کرده، تنها «انتشار» یا «افشای» داده‌های پزشکی نیست، بلکه وضعیت پیشینه‌تری است که می‌تواند مقدمه بروز آسیب‌های گسترده باشد: داشتن غیر مجاز یا نگهداری ناایمن داده‌های سلامت. در بسیاری از نظام‌های حقوقی پیشرفته، نهادهای نظارتی، از جمله اداره حقوق مدنی وزارت بهداشت آمریکا، کمیسر فدرال حفاظت از داده‌ها در آلمان، کمیسیون حفاظت از اطلاعات شخصی ژاپن و هیأت حفاظت از داده‌های اروپا در اسناد ۲۰۲۴ تا ۲۰۲۶ خود تأکید کرده‌اند که داشتن داده‌های سلامت، مادامی که بدون مجوز، بدون ضرورت حرفه‌ای یا خارج از استانداردهای امنیتی باشد، می‌تواند یک رفتار خطرزا تلقی گردد (۳).

این رویکرد جدید، نشانه گذار از سیاست کیفری واکنشی ـ که تنها پس از وقوع نشت داده یا آسیب مداخله می‌کرد ـ به سیاست کیفری پیشگیرانه و خطرمحور است. در این الگو، داشتن داده‌های پزشکی نه‌فقط به عنوان یک مسأله حقوقی، بلکه به عنوان یک موضوع مرتبط با امنیت اطلاعات، اعتماد به نظام درمانی و سلامت عمومی جامعه مطرح می‌شود (۴).

با این حال، در حقوق ایران با وجود پیشرفت‌هایی در حوزه جرائم رایانه‌ای و مقررات ناظر بر اسرار حرفه‌ای، هنوز تعریف حقوقی روشنی از «داشتن داده‌های پزشکی حساس» وجود ندارد. نه معیارهای احراز داشتن مشخص شده، نه مرز میان نگهداری مشروع و غیر مجاز تعیین شده و نه پیوند میان وضعیت داشتن و خطر بالقوه در حوزه سلامت دیجیتال تبیین گردیده است. این خلأ تقنینی باعث شده است ایران از قافله تحولات جهانی در سیاست کیفری داده‌های سلامت عقب بماند و نتواند پاسخی هماهنگ، منسجم و مبتنی بر اصول بنیادین به چالش‌های نوظهور ارائه دهد.

با توجه به گسترش زیرساخت‌های سلامت دیجیتال در ایران (پرونده الکترونیک سلامت، سامانه‌های نسخه‌نویسی دیجیتال، تبادل برخط داده‌های درمانی و ذخیره‌سازی ابری اطلاعات پزشکان و بیماران)، ضرورت دارد که نظام حقوق کیفری کشور نسبت به مسأله «داشتن غیر مجاز داده‌های پزشکی حساس» رویکردی علمی، دقیق و مبتنی بر تجارب نظام‌های موفق اتخاذ کند.

۱. بیان مسأله: با بررسی داده‌های پزشکی عصر حاضر، این پرسش به ذهن خطور می کند که آیا داشتن داده‌های پزشکی حساس ـ حتی بدون استفاده یا افشا ـ می‌تواند به عنوان یک رفتار مخاطره‌آمیز و تهدیدکننده سلامت دیجیتال، واجد مسئولیت کیفری باشد؟

این پرسش از چند جهت ابهام‌برانگیز است، چراکه حدود و ثغور مفهوم «داشتن» در حوزه داده مبهم است. داشتنِ داده، یک وضعیت فیزیکی نیست، بلکه وضعیت فنی ـ حقوقی پیچیده‌ای است. اینکه آیا ذخیره روی حافظه خارجی، داشتن محسوب می‌شود؟ آیا دسترسی موقت، به نوعی داشتن تلقی می‌شود؟ و یا شمول «دیتا لِیک‌ها» و «ابر» چگونه است؟

ماهیت داده‌های پزشکی حساس با سایر داده‌ها متفاوت است. این داده‌ها شامل ویژگی‌های زیستی، ژنتیکی، سلامت روان، بیماری‌های خاص و اطلاعات هویتی سلامت هستند (۲).

تمامی حقوق انتشار این اثر، متعلق به پژوهشکده اخلاق زیستی و حقوق سلامت پارس می‌باشد.

تحصیل، نگهداری یا انتقال این داده‌ها می‌تواند آسیب‌های طولانی‌مدت و بازگشت‌ناپذیر ایجاد کند.

ایران فاقد چارچوب تقنینی جامع و اختصاصی برای حمایت کیفری از داده‌های پزشکی حساس است، اگرچه قوانین موجود، از جمله قانون جرایم رایانه‌ای و مقررات حوزه سلامت، حمایت‌هایی را در این زمینه پیش‌بینی کرده‌اند، اما در تعریف داده‌های پزشکی حساس، تعیین مصادیق نگهداری و تصرف غیر مجاز و تبیین مسئولیت کیفری اشخاص دخیل در پردازش داده‌ها با خلأها و ابهاماتی مواجه‌اند. این مسأله در شرایطی پیچیده‌تر می‌شود که داده‌ها به صورت خودکار در اپلیکیشن‌ها ذخیره شوند، بدون آگاهی مستمر کاربر در فضای ابری باقی بمانند یا توسط شرکت‌های فناوری تحلیل شوند. از این رو تعیین حدود مداخله کیفری مستلزم بررسی ماهیت داده‌های پزشکی، مبانی جرم‌انگاری، ظرفیت‌های حقوق ایران و الگوهای بین‌المللی، با تأکید بر اصول قانونی‌بودن، ضرورت و تناسب جرم‌انگاری و حداقل‌گرایی کیفری است.

۲. اهمیت و ضرورت پژوهش: اهمیت این پژوهش از چند جنبه قابل تحلیل است: اهمیت سلامت دیجیتال در نظام‌های درمانی جدید، سلامت دیجیتال اکنون ستون فقرات نظام‌های سلامت است. گزارش سازمان توسعه و همکاری اقتصادی در سال ۲۰۲۵ بیان می‌کند که بیش از ۸۰ درصد تعاملات درمانی در جهان وابسته به داده‌های الکترونیک است (۵). بنابراین حفاظت کیفری از این داده‌ها، حفاظت از کل نظام سلامت است. افزایش تهدیدات زیست‌امنیتی و سایبری داده‌های پزشکی، به ویژه داده‌های ژنومی، در سال‌های اخیر هدف حملات سایبری گسترده قرار گرفته‌اند، زیرا ارزش سیاسی، اقتصادی و بیولوژیک دارند (۶).

آسیب‌پذیری شدید بیماران از نظر اطلاعاتی و فنی ضعیف هستند و امکان کنترل داده‌های خود را ندارند. بنابراین قانون باید حمایت ویژه‌ای ارائه دهد. خلأ تقنینی کامل در ایران ناشی از فقدان قانون جامع داده‌های پزشکی نظام مسئولیت کیفری برای داشتن غیر مجاز داده‌ها سازوکار نظارتی مستقل است. این خلأ می‌تواند به بحران‌های امنیتی و بهداشتی منجر شود. اهمیت برای سیاست‌گذاری و تصویب قوانین جدید نتایج این مقاله می‌تواند مبنای تدوین قانون حفاظت از داده‌های پزشکی اصلاح قانون جرائم رایانه‌ای تدوین آیین‌نامه‌های وزارت بهداشت باشد.

۳. مبانی نظری

۳-۱. مفهوم‌شناسی داده‌های پزشکی حساس: داده‌های پزشکی حساس (Sensitive Health Data) به اطلاعاتی اطلاق می‌شود که بیانگر وضعیت سلامت جسمی، روانی، ژنتیکی، بیومتریک یا سوابق درمانی افراد هستند و افشای آن‌ها می‌تواند به تبعیض، لطمه به حیثیت، آسیب روانی، یا سوءاستفاده گسترده منجر شود (۱). این دسته داده‌ها از منظر حقوقی، جزء بالاترین سطح طبقه‌بندی اطلاعات شخصی به شمار می‌آیند، زیرا نسبت به داده‌های معمولی، هم ارزش اطلاعاتی بالاتری دارند و هم پیامدهای آسیب‌پذیری آن‌ها شدیدتر است (۷).

بخش مهمی از حساسیت این داده‌ها ناشی از ماهیت آن‌ها نیست، بلکه از بافت اجتماعی ـ حرفه‌ای آن‌ها سرچشمه می‌گیرد، بدین‌معنا که داده پزشکی، علاوه بر کاربرد درمانی، حامل اعتمادِ بیمار به نظام سلامت است و نقض امنیت آن، مستقیماً اعتماد به پزشک، بیمارستان و حاکمیت را مخدوش می‌سازد (۸).

در اسناد سال‌های ۲۰۲۴ تا ۲۰۲۶، از جمله گزارش سازمان بهداشت جهانی و نظرات مقررات عمومی حفاظت از داده اتحادیه اروپا، بارها تأکید شده است که داده‌های سلامت باید صرفاً در بالاترین سطح امنیت فنی، مدیریتی و اخلاقی نگهداری شوند، زیرا حتی «نگهداری بدون مجوز» می‌تواند موجب بروز آسیب‌های بالقوه‌ای شود که عملاً مشابه آسیب‌های افشای بالفعل است (۹).

۳-۲. مبانی کیفری مفهوم داشتن داده‌های پزشکی: مفهوم «داشتن (Possession)» در حقوق کیفری کلاسیک، غالباً به حوزه اموال مادی تعلق داشت، اما با گسترش اقتصاد داده و ارزش فزاینده اطلاعات دیجیتال، این مفهوم به حوزه داده‌ها نیز تعمیم یافته است (۱۰). در حوزه داده‌های پزشکی،

تمامی حقوق انتشار این اثر، متعلق به پژوهشکده اخلاق زیستی و حقوق سلامت پارس می‌باشد

تصرف (Possession) به معنای توانایی واقعی یا بالقوه شخص برای دسترسی، کنترل، استخراج، ذخیره یا انتقال داده سلامت است، البته نکته مهم در تحلیل کیفری این مفهوم، تمایز میان داشتن فنی و داشتن حقوقی است.

داشتن فنی: صرف وجود داده در دستگاه، سرور یا حساب کاربری.

داشتن حقوقی: اختیار قانونی برای نگهداری، مشاهده یا استفاده از داده.

در برخی نظام‌های حقوقی، انتساب مسئولیت در قبال داده‌های سلامت با وضعیت دسترسی و نگهداری داده و وجود یا فقدان مجوز قانونی، نقش حرفه‌ای و ضرورت مرتبط با وظایف دارنده ارتباط دارد. برای نمونه، نظام استاندارد حفظ حریم خصوصی در ایالات متحده، مؤسسات مشمول را مکلف به اعمال کنترل‌های دسترسی و اتخاذ تدابیر اداری، فیزیکی و فنی برای حفاظت از اطلاعات سلامت الکترونیکی می‌کند. از منظر نظری نیز، تحول سیاست کیفری معاصر، توجه فزاینده‌ای به جرم‌انگاری رفتارهای واجد خطر و پیشگیری از آسیب پیش از تحقق زیان بالفعل نشان داده است، هرچند مشروعیت چنین مداخلاتی همچنان تابع اصول محدودکننده جرم‌انگاری است (۱۱-۱۰).

۳-۳. مبانی حقوق بشری حمایت از داده‌های پزشکی:

پایه‌های اصلی حمایت از داده‌های پزشکی را می‌توان در سه دسته حقوق بنیادین جستجو کرد:

دسته اول: حق بر حریم خصوصی مبتنی بر کرامت انسانی و آزادی کنترل اطلاعات شخصی؛

دسته دوم: حق بر سلامت که مستلزم امنیت اطلاعات درمانی و اعتماد بیمار به مراکز درمانی است؛

دسته سوم: حق بر خودمختاری اطلاعاتی که در نظام‌های نوین، یکی از اشکال حق بر تعیین سرنوشت فردی محسوب می‌شود.

در این چارچوب، داشتن غیر مجاز داده‌های پزشکی نوعی «تملک بر هویت اطلاعاتی فرد» تلقی می‌شود و از این جهت، حتی در صورت فقدان افشا، نقض اصل رضایت و کنترل فرد بر داده‌های خویش به شمار می‌آید (۱۲).

حقوق بشر مدرن در مواجهه با داده‌های سلامت، از مدل سنتیِ «محرمانگیِ پزشک ـ بیمار» به سمت مدل «حاکمیت داده‌های شخصی» حرکت کرده است. مبنای حقوق بشری این حمایت در اسناد بین‌المللی بر دو محور استوار است: حق بر حریم خصوصی و حق بر کرامت انسانی. در پارادایم کنونی (۲۶-۲۰۲۵ م.)، نگهداری داده‌های سلامت توسط اشخاص حقیقی یا حقوقی فاقد مجوز، نه‌تنها نقض حریم خصوصی، بلکه نقض «حقِ خودمختاری اطلاعاتی» تلقی می‌شود. طبق نظریات جدید در این حوزه، هر فرد حق دارد بر مسیر چرخش داده‌های بیومتریک و درمانی خود نظارت داشته باشد، چراکه هرگونه بهره‌برداری غیر مجاز از این داده‌ها، می‌تواند به «پروفایل‌سازی» و تبعیض‌های ساختاری علیه بیمار در حوزه‌های بیمه، استخدام یا دسترسی به خدمات اجتماعی منجر شود (۱۳).

تحولات حقوقی و رویکردهای نوین در حوزه حفاظت از داده‌های سلامت نشان می‌دهد نشان می‌دهد که نگهداری داده‌های پزشکی بدون «رضایت آگاهانه و مستمر»، عملاً به معنای استثمار داده‌ای فرد است. به تعبیر تحلیل‌گرانِ اخیر، داده‌های سلامت بخشی از «هویت دیجیتال» فرد محسوب می‌شوند و مداخله در آن‌ها، مداخله در کمالِ جسمانی و روانی انسان (۷، ۱۴). از این رو مسئولیت کیفری ناشی از «داشتن» غیر مجاز این داده‌ها، در واقع «ابزار حمایتی» برای صیانت از کرامت انسانی در برابر الگوریتم‌های پیش‌بین و کنترل‌گر است. این رویکرد حقوق بشری تأکید می‌کند که در نظام‌های مسئولیت‌پذیر، انتساب مسئولیت به دارندگان داده‌های سلامت باید با استانداردهای «امنیت‌محور» گره بخورد. به عبارت دیگر، هرگونه قصور در صیانت از این داده‌ها، مصداق نقض حقوق بنیادین بیمار است و جرم‌انگاریِ این فعل، واکنشی متناسب برای مهار ریسک‌های سیستماتیک در اکوسیستم سلامت دیجیتال می‌باشد (۱۰).

در عصر سلامت هوشمند، داده‌های پزشکی دیگر صرفاً «اطلاعاتی درباره بیماری» نیستند، بلکه «تصویر دیجیتال و بیولوژیک» فرد محسوب می‌شوند. گسترش این داده‌ها، مبانی

تمامی حقوق انتشار این اثر، متعلق به پژوهشکده اخلاق زیستی و حقوق سلامت پارس می‌باشد

نظری حقوق بشر را از حوزه «حریم خصوصی کلاسیک» به قلمرو «کرامت اطلاعاتی» سوق داده است.

۴. مبانی مبتنی بر نظریه حقوقی مدرن

۴-۱. داده‌های سلامت به مثابه بخشی از «بدن دیجیتال»: نظریه‌های حقوق بشری مدرن (۲۶-۲۰۲۵ م.) معتقدند که داده‌های سلامت، امتداد وجودیِ انسان در فضای سایبر هستند. اگر در حقوق سنتی، تعرض به جسم بیمار جرم‌انگاری شده است، در حقوق دیجیتال، دسترسی غیر مجاز به پرونده سلامت نیز نوعی «تعرض غیر فیزیکی» به تمامیت روانی و اجتماعی فرد است. بر این اساس، حمایت از این داده‌ها صرفاً یک ضرورت فنی نیست، بلکه تعهدی است مبتنی بر «حق بر کرامت انسانی»، هرگونه «داشتن» یا نگهداری غیر مجاز این داده‌ها توسط اشخاص غیر مسئول، به معنای تملک بخشی از هویت فردی است که می‌تواند زمینه را برای «پروفایل‌سازی» و ایجاد تبعیض‌های ساختاری در حوزه‌های بیمه، اشتغال و حتی تعاملات اجتماعی فراهم کند (۷، ۱۳).

۴-۲. گذار از حریم خصوصیِ منفی به «خودمختاری اطلاعاتی»: حق بر حریم خصوصی در اسناد و ادبیات معاصر حقوق بشر، از مفهوم سنتیِ «حق بر تنهاگذاشته‌شدن» فراتر رفته و به تدریج ابعاد ایجابی آن، از جمله حق فرد بر کنترل و تعیین سرنوشت اطلاعات شخصی خویش، مورد توجه قرار گرفته است. در حوزه سلامت، این تحول بدان‌معناست که بیمار باید تا حد امکان بر جمع‌آوری، نگهداری، پردازش و انتقال داده‌های سلامت خود کنترل داشته باشد. از این منظر، نگهداری یا پردازش داده‌های پزشکی بدون رضایت معتبر یا بدون وجود مبنای قانونی مشروع، می‌تواند نقض حق بر حریم خصوصی و خودمختاری اطلاعاتی فرد تلقی شود. چنین رویکردی، حمایت کیفری از داده‌های سلامت را نه صرفاً محدودیتی بر آزادی اشخاص، بلکه در شرایطی مشخص، ابزاری برای حمایت از استقلال، کرامت و کنترل اطلاعاتی بیمار در برابر سوءاستفاده از قدرت داده‌ای و مخاطرات ناشی از پردازش‌های الگوریتمی می‌داند (۱۴).

۴-۳. مسئولیت کیفری حمایتی: از دیدگاه حقوق بشری، مسئولیت کیفری در حوزه داده‌های سلامت نباید به ابزاری برای توسعه بی‌ضابطه قلمرو سرکوب کیفری تبدیل شود، بلکه باید در خدمت حمایت مؤثر از حریم خصوصی و حقوق بنیادین بیمار قرار گیرد. بر این اساس، جرم‌انگاری رفتار «داشتن» یا نگهداری غیر مجاز داده‌های پزشکی تنها در صورتی از مشروعیت سیاست جنایی برخوردار است که با اصول ضرورت، تناسب و پیشگیری از خطرهای قابل اعتنا سازگار باشد. در این چارچوب، شدت خطر، ماهیت و حساسیت داده، وضعیت و نقش دارنده، فقدان مجوز قانونی و احتمال سوءاستفاده یا افشای غیر مجاز، از جمله عواملی هستند که می‌توانند در تعیین حدود مسئولیت کیفری مؤثر باشند. چنین رویکردی، ضمن تقویت امنیت داده‌های سلامت، از تفسیر موسع عناوین مجرمانه و تبدیل هرگونه تخلف از الزامات حفاظت داده به جرم جلوگیری کرده و میان آزادی‌های علمی و درمانی از یک‌سو و ضرورت صیانت از حریم خصوصی و امنیت اطلاعات سلامت از سوی دیگر، تعادل برقرار می‌کند (۱۰).

می‌توان نتیجه‌گرفت از منظر حقوق بشری در نهایت «حق بر سلامت» در دنیای دیجیتال بدون «امنیتِ داده» بی‌معناست. اگر فرد بترسد که داده‌های پزشکی‌اش در اختیار اشخاص غیر مجاز (دارندگان غیر قانونی) قرار گیرد، از مشارکت در فرآیندهای درمانی و پژوهشی داده‌محور اجتناب خواهد کرد؛ اتفاقی که نه‌تنها حقوق فردی، بلکه «سلامت عمومی» جامعه را نیز تهدید می‌کند. بنابراین تدوین نظام کیفری دقیق برای جرم‌انگاری «داشتن غیر مجاز»، یک تکلیف حکومتی برای صیانت از حق بر سلامت و کرامت انسانی است.

۵. تحلیل نظری رابطه داشتن داده با ایجاد خطر:

نظریه‌های معاصر جرم‌انگاری پیشگیرانه، به ویژه در اثر «آشورث و زندر (Ashworth & Zedner)»، بر این نکته تأکید دارند که مداخله کیفری پیش از تحقق ضرر بالفعل، نیازمند توجیه مستقل و رعایت اصول محدودکننده‌ای همچون تناسب، قابلیت پیش‌بینی، فاصله معقول میان رفتار و زیان

تمامی حقوق انتشار این اثر، متعلق به پژوهشکده اخلاق زیستی و حقوق سلامت پارس می‌باشد

احتمالی و ضرورت مداخله کیفری است. در این رویکرد، صرف وجود یک وضعیت نامطلوب برای جرم‌انگاری کافی نیست، بلکه باید میان وضعیت مورد نظر و امکان تحقق آسیب، ارتباطی قابل توجیه وجود داشته باشد. در حوزه سلامت دیجیتال نیز گزارش سازمان ملی نوآوری اسپانیا در سال ۲۰۲۳ نشان می‌دهد که تهدید علیه داده‌های سازمان‌های سلامت از مهم‌ترین مخاطرات این حوزه است، به گونه‌ای که ۴۶ درصد از حوادث بررسی‌شده در این گزارش در قالب تهدید علیه داده‌ها قرار داشته و در ۵۲ مورد، از دست‌رفتن یا افشای داده‌های بیماران یا پرونده‌های الکترونیک سلامت گزارش شده است. از این رو نگهداری غیر مجاز داده‌های پزشکی، هنگامی که با ضعف کنترل‌های امنیتی، دسترسی‌های متعدد و فاقد نظارت، فقدان تدابیر حفاظتی متناسب یا امکان سوءاستفاده از داده‌ها همراه باشد، می‌تواند به عنوان یک وضعیت خطرزا در سیاست جنایی مورد توجه قرار گیرد. با این حال، وجود خطر فنی به تنهایی برای انتساب مسئولیت کیفری کافی نیست و جرم‌انگاری باید بر مبنای قانونی روشن، خطر قابل اعتنا، عنصر تقصیر یا سوءنیت مقرر در قانون و رعایت اصل تناسب استوار باشد (۱۰).

۶. مفهوم مشروعیت حرفه‌ای در نگهداری داده‌های پزشکی: در سیاست کیفری نوین، نگهداری داده فقط زمانی مشروع است که ضرورت حرفه‌ای یا درمانی وجود داشته باشد، نگهداری مطابق استاندارد امنیتی باشد، داده‌ها حداقلی و به‌روز باشند، مدت نگهداری متناسب و ناظر به هدف باشد.

در نظام‌هایی مانند آلمان، آمریکا و ژاپن، داشتن بیش از حد داده، نگهداری بلندمدت یا ذخیره‌سازی خارج از معماری رسمی، حتی اگر توسط یک حرفه‌مند انجام شود، می‌تواند به عنوان «داشتن غیر مجاز» تلقی شود (۱۵). این تحول مبتنی بر این اصل است که مشروعیت نگهداری داده، مطلق نیست و همیشه باید ناظر به هدف، ضرورت و امنیت باشد.

۶-۱. مفهوم مشروعیت حرفه‌ای در نگهداری داده‌های پزشکی: مشروعیت نگهداری داده‌های پزشکی، صرفاً با «وجود داده در اختیار یک شخص یا نهاد» تحقق نمی‌یابد، بلکه متکی بر مجموعه‌ای از معیارهای حقوقی، اخلاقی و حرفه‌ای است که وضعیت آن نگهداری را از «تصرف مجرمانه» متمایز می‌کند. در عصر سلامت دیجیتال که حجم عظیمی از داده‌های بیماران در سامانه‌های الکترونیک، پایگاه‌های ابری و پلتفرم‌های هوش مصنوعی جریان دارد، تفکیک میان نگهداری مشروع و نامشروع، اهمیت بنیادین برای تعیین قلمرو مسئولیت کیفری دارد (۱۷-۱۶).

۶-۲. عناصر سه‌گانه مشروعیت حرفه‌ای: می‌توان گفت نگهداری داده‌های پزشکی زمانی دارای مشروعیت حرفه‌ای است که حداقل سه عنصر به طور هم‌زمان فراهم باشد:

۶-۲-۱. پایه قانونی یا قراردادی روشن: نگهداری داده‌های پزشکی باید بر مبنای یک مستند حقوقی مشخص، از قبیل قانون، آیین‌نامه، مقررات حرفه‌ای یا تصمیم مقام صلاحیت‌دار یا بر اساس یک رابطه حقوقی معتبر میان دارنده و صاحب داده استوار باشد. در حوزه سلامت، این مبنا می‌تواند ناشی از رابطه درمانی، بیمه‌ای یا پژوهشی و در مواردی ناشی از تکلیف قانونی به نگهداری سوابق پزشکی باشد. برای نمونه، پزشک یا مرکز درمانی ممکن است بر اساس الزامات قانونی و حرفه‌ای مکلف به ثبت و نگهداری پرونده بیمار برای مدت مقرر باشد؛ در چنین وضعیتی، «داشتن» داده نه‌تنها فاقد وصف نامشروع است، بلکه بخشی از ایفای وظیفه حرفه‌ای و قانونی محسوب می‌شود. در مقابل، شخص یا نهادی که فاقد مبنای قانونی، رابطه قراردادی معتبر یا رضایت و مجوز لازم برای دسترسی و نگهداری اطلاعات بیمار است، نمی‌تواند صرفاً با استناد به در اختیارداشتن فیزیکی یا فنی داده، مشروعیت نگهداری آن را توجیه کند. بنابراین وجود «مبنای معتبر نگهداری» یکی از معیارهای اساسی برای تفکیک نگهداری مشروع از نگهداری غیر مجاز و در موارد مقرر، تعیین حدود مسئولیت حقوقی و کیفری است (۱۸-۱۷).

۶-۲-۲. هدف درمانی، پژوهشی یا مدیریتی مشروع و مشخص: مشروعیت نگهداری داده‌های پزشکی، علاوه بر وجود مبنای قانونی یا رضایت معتبر، با هدف و غایت مشخصِ پردازش و نگهداری ارتباط مستقیم دارد. نگهداری داده

تمامی حقوق انتشار این اثر، متعلق به پژوهشکده اخلاق زیستی و حقوق سلامت پارس می‌باشد

هنگامی از منظر حرفه‌ای و حقوقی موجه است که در راستای اهداف مشروعی همچون ارائه خدمات درمانی، مدیریت نظام سلامت، انجام پژوهش‌های علمی و اخلاق‌مدار، ارتقای کیفیت مراقبت یا سایر اهداف قانونی و معین صورت گیرد. در مقابل، استفاده از داده‌های سلامت برای اهدافی نظیر تبلیغات نامرتبط، بهره‌برداری تجاری ناموجه، کنترل غیر ضروری یا ایجاد تبعیض، در صورتی که فاقد مبنای قانونی و تضمین‌های لازم باشد، می‌تواند مشروعیت پردازش و نگهداری داده را با تردید جدی مواجه سازد (۱۹).

در حوزه استفاده ثانویه از داده‌های سلامت نیز اصل بر آن است که پردازش داده باید در چارچوب یک مبنای قانونی معتبر و سازوکارهای مناسب حکمرانی داده انجام شود. سازمان توسعه و همکاری اقتصادی در گزارش سال ۲۰۲۵ خود بر ضرورت وجود چارچوب‌های حکمرانی، تعیین روشن اهداف و مسئولیت‌ها، مدیریت ریسک و ایجاد محیط‌های قابل اعتماد برای استفاده ثانویه از داده‌های سلامت تأکید کرده است (۱۹). همچنین استفاده پژوهشی از داده‌های شخصی، حسب مبنای حقوقی حاکم، می‌تواند مستلزم رضایت یا مبنای قانونی جایگزین، سازوکارهای نظارت و تأیید اخلاقی و اتخاذ تدابیر مناسب برای کاهش خطر شناسایی مجدد باشد (۲۱-۲۰). بنابراین مشروعیت «داشتن» داده پزشکی را نمی‌توان صرفاً از انتساب آن به یک نهاد حرفه‌ای استنباط کرد، بلکه باید هدف، مبنای حقوقی، ضرورت، حدود استفاده و تدابیر حفاظتی مربوط به آن نیز احراز شود.

۶-۲-۳. رعایت استانداردهای حرفه‌ای و امنیتی: مشروعیت حرفه‌ای نگهداری داده‌های پزشکی صرفاً از عنوان یا موقعیت شغلی دارنده داده، مانند پزشک یا مدیر مؤسسه درمانی، ناشی نمی‌شود، بلکه مستلزم رعایت مجموعه‌ای از الزامات حقوقی و حرفه‌ای در زمینه محرمانگی، کنترل دسترسی، تمامیت و امنیت اطلاعات است. در نظام‌های نوین حفاظت از داده‌های سلامت، دارنده اطلاعات مکلف است متناسب با ماهیت داده و میزان خطر، تدابیر اداری، فنی و فیزیکی مناسب را برای جلوگیری از دسترسی یا افشای غیر مجاز اتخاذ کند (۷). برای نمونه، مقررات امنیتی استاندارد حفظ حریم خصوصی بر کنترل دسترسی، احراز هویت، ثبت و ممیزی فعالیت‌های سامانه و اتخاذ تدابیر امنیتی متناسب با ارزیابی ریسک تأکید دارد؛ در این چارچوب، رمزنگاری نیز حسب ارزیابی ریسک می‌تواند به عنوان یک تدبیر امنیتی لازم مطرح شود (۱، ۴، ۷، ۱۱).

بنابراین، حتی در فرضی که اصل نگهداری داده توسط پزشک یا مؤسسه درمانی دارای مبنای قانونی باشد، عدم رعایت الزامات امنیتی و حرفه‌ای می‌تواند موجب نقض تکالیف قانونی و انتظامی و در صورت تحقق شرایط مقرر در قانون، مسئولیت مدنی یا کیفری شود. با این حال، صرف ضعف امنیتی یا عدم استفاده از یک فناوری خاص، به تنهایی برای انتساب مسئولیت کیفری کافی نیست و تحقق مسئولیت کیفری مستلزم وجود نص قانونی و احراز سایر عناصر و شرایط جرم است (۱۱).

۶-۳. تمایز میان نگهداری حرفه‌ای و نگهداری شخصی یا تجاری: یکی از چالش‌های اساسی در سیاست کیفری سلامت دیجیتال، تفکیک دقیق نگهداری حرفه‌ای از نگهداری شخصی یا تجاری است.

ـ در نگهداری حرفه‌ای، داده‌ها در چارچوب یک سازمان یا فرد دارای صلاحیت (مثل پزشک، بیمارستان، مرکز پژوهشی دارای مجوز) و برای انجام وظایف مشخص حرفه‌ای نگهداری می‌شوند. این نوع نگهداری معمولاً تحت نظارت نهادهای حرفه‌ای، وزارت بهداشت یا مراجع ناظر بر حریم خصوصی است.

ـ در نگهداری شخصی یا تجاری، داده‌های سلامت ممکن است توسط افراد، شرکت‌ها یا پلتفرم‌هایی نگهداری شوند که نه رابطه درمانی رسمی با فرد دارند، نه تحت نظم حرفه‌ای مشخصی فعالیت می‌کنند، مانند اپلیکیشن‌های غیر استاندارد، کارگزاران داده یا اشخاصی که داده‌ها را از طریق نشت اطلاعات یا خرید غیر قانونی به دست آورده‌اند (۲۲).

نظام‌های حقوقی پیشرو، مشروعیت و ضرورت حرفه‌ای پردازش و نگهداری داده‌های شخصی را منوط به وجود مبنای قانونی، هدف مشخص و رعایت اصول ضرورت، تناسب، امنیت و محدودیت هدف می‌دانند. بنابراین نگهداری داده در

تمامی حقوق انتشار این اثر، متعلق به پژوهشکده اخلاق زیستی و حقوق سلامت پارس می‌باشد

چارچوب فعالیت حرفه‌ای، مادامی که در حدود وظایف و ضرورت حرفه‌ای باقی بماند، از نگهداری فاقد مبنای قانونی و اهداف فرعی نامشروع متمایز می‌شود.

۶-۴. حدود و ثغور مشروعیت حرفه‌ای: ضرورت، تناسب و حداقل‌سازی داده: برای جلوگیری از تبدیل «مشروعیت حرفه‌ای» به یک عنوان کلی و قابل سوءاستفاده، لازم است سه معیار: ۱ـ ضرورت؛ ۲ـ تناسب؛ ۳ـ حداقل‌سازی داده، در قانون یا راهنماهای حرفه‌ای تصریح شود:

۶-۴-۱. ضرورت: نگهداری داده باید به میزان لازم برای تحقق هدف مشروع انجام شود. اگر داده‌ای برای درمان، پیگیری وضعیت بیمار یا انجام پژوهش ضروری نیست، نگهداری آن در چارچوب حرفه‌ای موجه نخواهد بود. این معیار، مانع جمع آوری و انباشت بی‌ضابطه داده‌های مازاد بر نیاز حرفه‌ای می‌شود (۱۴).

۶-۴-۲. تناسب: حتی در موارد ضروری، دامنه و مدت نگهداری باید متناسب با هدف باشد، مثلاً نگهداری مادام‌العمر داده‌های ظریف و بسیار حساس برای یک بیماری جزئی، بدون ضرورت پزشکی، می‌تواند از منظر حقوق بشری و حرفه‌ای نامشروع تلقی شود. معیار تناسب، افراط در نگهداری و تبدیل پایگاه‌های داده به «آرشیو دائمی آسیب‌پذیری‌های فرد» را محدود می‌کند (۲۳).

۶-۴-۳. حداقل‌سازی داده: اصل حداقل‌سازی که در اسناد بین‌المللی به صورت گسترده پذیرفته شده است، اقتضا می‌کند که صرفاً داده‌هایی نگهداری شوند که برای هدف حرفه‌ای ضروری هستند و امکان شبه‌ناشناس‌سازی یا رمزنگاری آن‌ها نیز بررسی و اجرا شود. رعایت این اصل، هم مشروعیت حرفه‌ای را تقویت می‌کند و هم احتمال تحقق مسئولیت کیفری ناشی از نشت یا سوءاستفاده از داده را کاهش می‌دهد (۲۴).

۶-۵. مسئولیت حرفه‌ای و نقش آن در تحدید مسئولیت کیفری: یکی از کارکردهای مهم مفهوم «مشروعیت حرفه‌ای» در نگهداری داده‌های پزشکی، تحدید دایره مسئولیت کیفری و جلوگیری از جرم‌انگاری بی‌رویه است. هنگامی که قانون‌گذار معیارهای روشن مشروعیت حرفه‌ای را تعریف کند:

ـ از یک‌سو، پزشکان، پرستاران، مدیران سامانه‌های سلامت و پژوهشگران می‌توانند با اتکا به این معیارها، فعالیت خود را سامان داده و از قرارگرفتن در معرض اتهام‌های کیفری ناموجه مصون بمانند؛

ـ از سوی دیگر، امکان تعقیب کیفری افرادی که به صورت آگاهانه خارج از حدود حرفه‌ای و بدون رعایت استانداردها، داده‌های پزشکی را نگهداری می‌کنند، تسهیل می‌شود.

در این چارچوب، مسئولیت حرفه‌ای (انتظامی و مدنی) نقش پیشینی دارد و مسئولیت کیفری به عنوان «آخرین واکنش» در موارد نقض فاحش، سازمان‌یافته یا خطرزای استانداردهای حرفه‌ای اعمال می‌شود. این رویکرد با الگوی «خطرمحور محدود» در سیاست کیفری داده‌های سلامت هم‌خوانی دارد و مانع از آن می‌شود که هر نقض کوچک حرفه‌ای به سطح جرم کیفری ارتقا یابد (۱۰).

۶-۶. جمع‌بندی: ضرورت تصریح مفهوم مشروعیت حرفه‌ای در حقوق ایران: در حقوق ایران، هرچند مقرراتی درباره محرمانگی پزشکی، اسرار شغلی و جرائم رایانه‌ای وجود دارد، اما مفهوم «مشروعیت حرفه‌ای در نگهداری داده‌های پزشکی» به صورت صریح و منسجم تعریف نشده است. این خلأ موجب می‌شود که: از یک‌سو، ارائه‌دهندگان خدمات سلامت و پژوهشگران در مرز باریک میان تکلیف حرفه‌ای به نگهداری داده و خطر مسئولیت کیفری ناشی از اتهام «نگهداری غیر مجاز» حرکت کنند و از سوی دیگر، افرادی که عملاً خارج از هر چارچوب حرفه‌ای و بدون هرگونه توجیه مشروع، داده‌های حساس بیماران را در اختیار دارند، گاه با استفاده از ابهام‌های قانونی از پاسخگویی کیفری می‌گریزند.

بنابراین یکی از پیشنهادهای تقنینی مهم آن است که قانون‌گذار در قالب قانون خاص «حمایت از داده‌های سلامت» یا اصلاح قوانین موجود، تعریف دقیق و معیارهای مشروعیت حرفه‌ای در نگهداری داده‌های پزشکی را پیش‌بینی کند. این تعریف باید به روشنی، مواردی را که نگهداری داده در

تمامی حقوق انتشار این اثر، متعلق به پژوهشکده اخلاق زیستی و حقوق سلامت پارس می‌باشد

چارچوب حرفه‌ای و با هدف مشروع انجام می‌شود از مواردی که نگهداری ماهیتاً خطرزا، تجاری یا سوءاستفاده‌گرانه دارد، تفکیک نماید. چنین رویکردی، هم امنیت حقوقی فعالان نظام سلامت را تقویت می‌کند و هم امکان اعمال مؤثر مسئولیت کیفری علیه دارندگان غیر مجاز داده‌های پزشکی را فراهم می‌آورد (۲۷-۲۵).

۷. پیوند میان داشتن داده و مسئولیت کیفری: در نهایت، گذار از مسئولیت مبتنی بر رفتار به مسئولیت مبتنی بر وضعیت، زمانی موجه است که وضعیت مورد نظر واجد ظرفیت جرم‌زا باشد، قابلیت کنترل فردی داشته باشد و عدم مداخله قانون موجب افزایش احتمال تحقق آسیب جدی شود. در سیاست کیفری سلامت، نگهداری غیر مجاز داده‌های پزشکی، با توجه به ماهیت حساس این داده‌ها و پیامدهای بالقوه ناشی از دسترسی، افشا یا سوءاستفاده از آن‌ها، می‌تواند در چارچوب سیاست کیفری پیشگیرانه مورد توجه قرار گیرد. با این حال، جرم‌انگاری چنین وضعیتی باید با رعایت اصل قانونی‌بودن جرم و مجازات، اصل تناسب و ضرورت مداخله کیفری صورت گیرد تا صرف «داشتن» داده، بدون احراز شرایط لازم برای تحقق مسئولیت کیفری، موجب توسعه ناموجه قلمرو حقوق کیفری نشود. این مبانی نظری، زیربنای بخش‌های تطبیقی و تحلیل چالش‌های حقوق ایران را تشکیل می‌دهد (۲۸).

حقوق بشر مدرن در مواجهه با داده‌های سلامت، از مدل سنتی «محرمانگی پزشک ـ بیمار» به سمت الگوی گسترده‌تر «حفاظت و حاکمیت بر داده‌های شخصی» حرکت کرده است. در این چارچوب، حمایت از داده‌های سلامت نه‌تنها به رابطه حرفه‌ای پزشک و بیمار محدود نمی‌شود، بلکه حق فرد بر کنترل اطلاعات شخصی، حمایت از حریم خصوصی و صیانت از شخصیت و کرامت انسانی را نیز دربر می‌گیرد (۱۰، ۱۴). از این منظر، داده‌های پزشکی را می‌توان بخشی از قلمرو اطلاعات خصوصی فرد دانست که دسترسی، جمع‌آوری، پردازش و افشای آن‌ها، جز در موارد دارای مبنای قانونی و مشروع، می‌تواند با حق بر حریم خصوصی و کرامت انسانی تعارض پیدا کند.

۷-۱. ظهور حوزه جدیدی از مسئولیت کیفری داده: تحولات فناوری در پنج سال اخیر به ویژه با ورود هوش مصنوعی مولد و اینترنتِ اشیای پزشکی، باعث ظهور نوعی «مسئولیت کیفری داده‌محور» شده است. در این چارچوب، دیگر صرفِ انجام فعل سنتیِ جرم‌انگارانه (مانند سرقت یا افشا) معیار انتساب مسئولیت نیست (۲۹)، بلکه «وضعیت داشتن داده حساس»، به عنوان یک شرط خطرزای کیفری در نظر گرفته می‌شود. نگهداری داده‌های سلامت بدون مجوز، حتی اگر همراه با قصد سوءاستفاده نباشد، به خودی خود می‌تواند مصداق ایجاد خطر برای حقوق بنیادین افراد تلقی شود (۳۰).

به بیان دیگر، در حقوق کیفری داده، مسئولیت کیفری از «رفتار» به سمت «وضعیت» جا به جا شده است، یعنی مسئولیت ناشی از «داشتن» داده، زمانی تحقق می‌یابد که آن نگهداری باعث ایجاد احتمال واقعیِ نقض حریم خصوصی یا آسیب به سلامت افراد گردد.

۷-۲. مفهوم «داشتن» در فضای داده‌محور: از تصرف فیزیکی تا کنترل اطلاعاتی: در فضای دیجیتال، مفهوم تصرف (Possession) دیگر به معنای داشتن فیزیکی نیست، بلکه عبارت است از توانایی آگاهانه برای کنترل، دسترسی یا بهره‌برداری از داده. بنابراین داشتن داده‌های پزشکی به صورت واقعی زمانی محقق است که شخص:

۱ـ از وجود داده‌های حساس آگاه باشد؛

۲ـ بتواند به آن‌ها به طور مؤثر دسترسی پیدا کند؛

۳ـ اختیار فنی یا سازمانی برای استفاده، انتقال یا افشا داشته باشد.

این تفسیر در نظریات جدید حقوق کیفری داده‌ها به عنوان «سلطه اطلاعاتی» شناخته می‌شود. به تعبیر «آشورث و زندر» شخصی که چنین سلطه‌ای را اعمال می‌کند، در واقع «دارنده بالقوه خطر» است و از این رو باید در حدودی مشخص مسئولیت کیفری داشته باشد، حتی اگر هنوز عملی سوء انجام نداده باشد (۱۰).

تمامی حقوق انتشار این اثر، متعلق به پژوهشکده اخلاق زیستی و حقوق سلامت پارس می‌باشد

۸. مبانی انتساب مسئولیت کیفری در داشتن داده‌های سلامت: در نظام‌های نوین حقوقی، انتساب مسئولیت کیفری ناشی از داشتن داده، مبتنی بر سه مبنا صورت می‌گیرد:

۸-۱. مبنای خطر: این رویکرد، داده‌های سلامت را به دلیل ماهیت بسیار حساس و پیامدهای بالقوه ناشی از دسترسی یا استفاده غیر مجاز، در زمره داده‌هایی قرار می‌دهد که نگهداری و پردازش آن‌ها مستلزم رعایت الزامات دقیق حفاظتی است. در چارچوب فضای اروپایی داده‌های سلامت، مقرره جدید اتحادیه اروپا، مجموعه‌ای از الزامات را برای دارندگان و استفاده‌کنندگان داده‌های سلامت مقرر کرده و دسترسی و استفاده ثانویه از این داده‌ها را به سازوکارهای نظارتی، مجوزهای دسترسی و محیط‌های پردازش امن مشروط ساخته است. همچنین استفاده‌هایی مانند بازشناسایی اشخاص، تبعیض یا دسترسی اشخاص ثالث فاقد مجوز به داده‌های سلامت ممنوع شده است (۳۱). این تحولات نشان می‌دهد که در نظام‌های جدید حکمرانی داده، صرف برخورداری از داده‌های سلامت، بدون توجه به نحوه کنترل، دسترسی و حفاظت از آن‌ها، نمی‌تواند از منظر حقوقی خنثی تلقی شود، بلکه نوع و میزان کنترل بر داده و خطر ناشی از نقض حقوق صاحبان داده، در تعیین حدود مسئولیت حقوقی و نظارتی اهمیت فزاینده‌ای یافته است.

۸-۲. مبنای اعتماد عمومی: پزشکی و نظام درمانی تا حد زیادی بر پایه اعتماد میان بیمار و ارائه‌دهندگان خدمات سلامت شکل گرفته است. بیمار برای دریافت خدمات درمانی ناگزیر است اطلاعاتی بسیار شخصی و حساس را در اختیار پزشک و سایر اشخاص دخیل در فرایند درمان قرار دهد و انتظار مشروع دارد این اطلاعات صرفاً در حدود قانونی و حرفه‌ای مورد استفاده قرار گیرد. از این منظر، محرمانگی اطلاعات سلامت نه‌تنها یکی از الزامات اخلاق حرفه‌ای، بلکه یکی از پایه‌های شکل‌گیری و استمرار اعتماد در رابطه پزشک ـ بیمار است. سازمان جهانی پزشکی نیز بر این نکته تأکید کرده است که محرمانگی برای حفظ اعتماد و یکپارچگی پایگاه‌های داده سلامت ضروری است و اشخاصی که اطلاعات بیماران را در اختیار دارند، در قبال حفاظت از آن‌ها دارای مسئولیت اخلاقی و حقوقی هستند. بنابراین نگهداری، استفاده یا افشای غیر مجاز داده‌های سلامت می‌تواند اعتماد بیماران به نظام درمانی را تضعیف کرده و مبنایی برای توجیه مداخله حقوقی و در موارد واجد شرایط، جرم‌انگاری رفتارهای پرخطر در این حوزه فراهم آورد (۷).

۸-۳. مبنای تکلیف حرفه‌ای: در این مبنا، مسئولیت دارنده داده صرفاً ناشی از یک ممنوعیت عام قانونی نیست، بلکه از تکلیف حرفه‌ای و سازمانیِ ناشی از موقعیت وی نسبت به داده‌های سلامت نیز سرچشمه می‌گیرد. پزشکان، پژوهشگران، مؤسسات درمانی و سایر اشخاصی که به اقتضای حرفه یا وظیفه سازمانی به داده‌های حساس سلامت دسترسی دارند، مکلف‌اند این داده‌ها را مطابق الزامات محرمانگی، امنیت و حفاظت از داده‌ها مدیریت کنند. در حقوق آلمان، برای اشخاص مشمول اسرار حرفه‌ای پزشکی، نقض تکلیف محرمانگی می‌تواند واجد ضمانت اجرای کیفری باشد؛ همچنین در نظام ژاپن نیز مقررات مربوط به حفاظت از اطلاعات شخصی و اسرار حرفه‌ای، برای برخی اشکال استفاده یا افشای غیر مجاز از اطلاعات، مسئولیت و ضمانت اجرای قانونی پیش‌بینی کرده است. بنابراین مبنای تکلیف حرفه‌ای می‌تواند یکی از پایه‌های تحلیل مسئولیت کیفری در حوزه داده‌های سلامت باشد، هرچند تحقق مسئولیت کیفری منوط به وجود نص قانونی، رفتار ممنوع و سایر عناصر لازم جرم است و صرف عدم رعایت یک دستورالعمل حفاظتی، بدون وجود مبنای قانونی کافی، الزاماً جرم محسوب نمی‌شود (۳۲).

۹. تطبیق نظریه‌ها در نظام‌های حقوقی پیشرو: بررسی تطبیقی نظام‌های حقوقی پیشرو نشان می‌دهد که مسئولیت ناشی از کنترل داده‌های سلامت، در تقاطع میان حفاظت از داده، تکالیف حرفه‌ای و رویکردهای نوین مبتنی بر خطر شکل گرفته است.

۹-۱. اتحادیه اروپا: در اتحادیه اروپا، چارچوب حقوقی حفاظت از داده‌های سلامت عمدتاً بر حفاظت پیشینی، محدودیت دسترسی، امنیت پردازش و مدیریت خطر برای

تمامی حقوق انتشار این اثر، متعلق به پژوهشکده اخلاق زیستی و حقوق سلامت پارس می‌باشد

حقوق و آزادی‌های اشخاص استوار است. مقررات عمومی حفاظت از داده اتحادیه اروپا داده‌های مربوط به سلامت را در زمره داده‌های دارای حساسیت ویژه قرار داده و برای پردازش آن‌ها شرایط و تضمین‌های خاصی مقرر می‌کند. همچنین مقررات فضای اروپایی داده‌های سلامت با تقویت سازوکارهای کنترل دسترسی و استفاده ثانویه از داده‌های سلامت، مسئولیت‌های دارندگان و استفاده‌کنندگان این داده‌ها را افزایش داده است. بنابراین در حقوق اتحادیه اروپا می‌توان نگهداری و کنترل غیر مجاز داده‌های سلامت را در چارچوب نقض الزامات حفاظت از داده و ایجاد خطر برای حقوق اشخاص تحلیل کرد؛ با این حال، تبدیل این وضعیت به جرم مستقل صرفِ «داشتن داده» نیازمند مبنای کیفری مشخص در حقوق داخلی دولت عضو است و صرف مقررات یاد شده، چنین جرم مستقلی ایجاد نمی‌کند (۳۳).

۹-۲. ایالات متحده: در ایالات متحده، نظام استاندارد حفظ حریم خصوصی برای اشخاص و نهادهای مشمول، الزامات مشخصی در زمینه حفاظت، امنیت و افشای اطلاعات سلامت مقرر کرده است. نقض برخی الزامات نظام استاندارد حفظ حریم خصوصی، به ویژه در مواردی که با آگاهی و شرایط مقرر قانونی صورت گیرد، می‌تواند ضمانت اجرای کیفری داشته باشد. با این حال، صرف نگهداری ناامن داده‌های سلامت، بدون تحقق شرایط مقرر در قانون، به طور کلی جرم مستقل محسوب نمی‌شود. بنابراین در تحلیل حقوق آمریکا باید میان تخلف از الزامات امنیتی و حریم خصوصی، مسئولیت اداری و مدنی، و مسئولیت کیفری ناشی از رفتارهای عمدی و ممنوع تمایز قائل شد (۳۴).

۹-۳. آلمان و ژاپن: در آلمان و ژاپن نیز حمایت از محرمانگی و امنیت داده‌های سلامت با تکالیف حرفه‌ای و الزامات قانونی حفاظت از داده‌ها پیوند خورده است. در ژاپن، اطلاعات مربوط به وضعیت جسمانی، بیماری، نتایج معاینه و درمان در شمار اطلاعاتی قرار می‌گیرند که مستلزم حمایت ویژه هستند و برای اشخاص و مؤسسات درمانی تکالیف مشخصی در زمینه مدیریت و حفاظت از آن‌ها پیش‌بینی شده است. در صورت نقض برخی تکالیف قانونی، بسته به نوع رفتار و شرایط قانونی، ضمانت اجراهای اداری و در موارد مقرر، کیفری نیز قابل تصور است. از این رو، در این نظام‌ها نیز مبنای مسئولیت را باید در نقض تکلیف قانونی یا حرفه‌ای مشخص جست‌وجو کرد، نه صرف وضعیت فیزیکی یا دیجیتالِ داشتن داده (۳۶-۳۵).

۱۰. دیدگاه‌های نوین جرم‌انگاری داده در سال‌های ۲۶-۲۰۲۵: در ادبیات نوین حقوق داده و حقوق کیفری، تحولات فناوری و گسترش هوش مصنوعی، داده‌های سلامت و سامانه‌های دیجیتال موجب تقویت رویکردهای پیشگیرانه و مبتنی بر مدیریت خطر شده است. با این حال، این تحول لزوماً به معنای جرم‌انگاری صرفِ «داشتن داده» نیست، بلکه بر ضرورت شناسایی و کنترل خطرهای ناشی از دسترسی، پردازش و نگهداری داده‌های حساس تأکید دارد.

۱۰-۱. حرکت از جرم‌انگاری نتیجه به جرم‌انگاری خطر: در محیط‌های دیجیتال، به ویژه در حوزه سلامت، حجم گسترده داده‌های حساس و وابستگی فزاینده نظام درمانی به زیرساخت‌های دیجیتال، اهمیت پیشگیری از نقض امنیت و حریم خصوصی را افزایش داده است. گزارش‌های جدید سازمان توسعه و همکاری اقتصادی نشان می‌دهند که گسترش هوش مصنوعی در سلامت، هم‌زمان با فرصت‌های مهم، خطرهای مرتبط با حریم خصوصی، امنیت داده و ضعف نظارت را نیز افزایش داده است. همچنین سازمان ملی نوآوری اسپانیا، در ارزیابی تهدیدهای بخش سلامت، نقض داده و حملات سایبری را از مهم‌ترین تهدیدهای این حوزه معرفی کرده است (۳۰).

۱۰-۲. حرکت به سوی حفاظت پیشینی از داده: در رویکردهای جدید حکمرانی داده، حفاظت از داده دیگر صرفاً به مرحله وقوع افشا یا ورود خسارت محدود نمی‌شود، بلکه کنترل دسترسی، محدودسازی استفاده، امنیت داده، مدیریت خطر بازشناسایی و سازوکارهای حکمرانی از مراحل اولیه پردازش مورد توجه قرار می‌گیرند. برخی از نهادهای ذی‌ربط در چارچوب حکمرانی داده‌های سلامت بر ایجاد سازوکارهایی

تمامی حقوق انتشار این اثر، متعلق به پژوهشکده اخلاق زیستی و حقوق سلامت پارس می‌باشد

برای حفاظت از حریم خصوصی و امنیت داده و مدیریت خطرهای ناشی از دسترسی و استفاده از داده‌های سلامت تأکید کرده است (۱۰).

۱۰-۳. اعمال مسئولیت متناسب با سطح کنترل: یکی از نتایج مهم این رویکرد آن است که مسئولیت نباید بدون توجه به میزان اختیار، دسترسی و قدرت واقعی شخص بر داده به طور یکسان بر تمام کاربران تحمیل شود. در نظام‌های نوین حکمرانی داده، میان دارنده یا متولی اصلی داده، شخص دارای اختیار تصمیم‌گیری درباره پردازش و کاربران محدود یا فاقد اختیار مؤثر باید تفکیک ایجاد شود. چنین تمایزی با اصول دسترسی کنترل‌شده، حداقل‌سازی دسترسی و مدیریت ریسک در حکمرانی داده‌های سلامت سازگار است. سازمان توسعه و همکاری اقتصادی نیز بر اهمیت کنترل دسترسی، آموزش کارکنان، مدیریت خطر بازشناسایی و حفاظت از داده‌ها هنگام اتصال و دسترسی تأکید کرده است (۳۷).

۱۱. تحلیل تطبیقی: تحلیل تطبیقی در این پژوهش صرفاً به معنای توصیف مقررات چند نظام حقوقی نیست، بلکه هدف اصلی آن استخراج الگوهای غالب، تفاوت‌های ساختاری و منطق سیاست کیفریِ حاکم بر جرم‌انگاری یا عدم جرم‌انگاری نگهداری داده‌های پزشکی حساس است. از این منظر، مقایسه نظام‌های منتخب نشان می‌دهد که مسأله «داشتن» داده در محیط دیجیتال، در حقوق کیفری معاصر به تدریج از یک تصور صرفاً فیزیکی فاصله گرفته و به سمت فهمی مبتنی بر آگاهی، دسترسی مؤثر و امکان کنترل حرکت کرده است، در نتیجه، ارزیابی تطبیقی باید نه فقط بر متن قوانین، بلکه بر فلسفه تنظیم‌گری، میزان مداخله کیفری و نسبت میان ابزارهای کیفری، اداری و فنی متمرکز شود (۳۰).

این رویکرد با این پیش‌فرض همراه است که جرم‌انگاری در حوزه داده‌های سلامت، به ویژه در مورد «صرف نگهداری»، تنها زمانی موجه است که سازوکارهای غیر کیفری قادر به مهار خطر نباشند و رفتار مزبور واجد درجه‌ای از خطر واقعی و قابل انتساب برای حقوق اشخاص باشد (۱۰).

۱۱-۱. اتحادیه اروپا: تقدم حکمرانی داده بر مداخله کیفری: در اتحادیه اروپا، الگوی غالب در حوزه حفاظت از داده‌های سلامت، بیش از آنکه بر توسعه ضمانت‌اجراهای کیفری استوار باشد، بر حکمرانی داده، شفافیت پردازش، پاسخگویی سازمانی، محدودیت هدف، امنیت پردازش و تضمین حقوق اشخاص متمرکز است. این رویکرد را می‌توان در منطق حاکم بر مقررات عمومی حفاظت از داده و نیز در تحولات مربوط به فضای اروپایی داده‌های سلامت مشاهده کرد. در این چارچوب، هدف اصلی ایجاد یک معماری حقوقی منسجم برای تنظیم جمع‌آوری، پردازش، دسترسی و استفاده مجدد از داده‌های سلامت و در عین حال تضمین حقوق بنیادین اشخاص است. مقررات اتحادیه اروپا نیز به جای اتکا به یک پاسخ کیفری واحد، مجموعه‌ای از الزامات پیشینی، اقدامات اصلاحی و ضمانت‌اجراهای اداری را پیش‌بینی کرده و در عین حال، مقرر می‌کند که دولت‌های عضو می‌توانند برای برخی نقض‌ها ضمانت‌اجراهای کیفری مقرر کنند. بنابراین پاسخ کیفری در این نظام عمدتاً در چارچوب حقوق ملی دولت‌های عضو تکمیل می‌شود (۱۰، ۳۰).

این ویژگی نشان می‌دهد که سیاست تقنینی اتحادیه اروپا در حوزه داده‌های سلامت، تا حد زیادی از منطق «پیشگیری ساختاری» پیروی می‌کند. به جای آنکه صرف نگهداری داده حساس، مستقلاً و در همه شرایط موضوع جرم قرار گیرد، نظام تنظیمی اروپا بر ایجاد الزامات پیشینی برای کنترل دسترسی، امنیت پردازش، تعیین هدف، حداقل‌سازی داده، پاسخگویی و ارزیابی خطر تمرکز دارد. در فضای اروپایی داده‌های سلامت نیز بر ایجاد سازوکارهای حکمرانی، دسترسی کنترل‌شده، مجوزهای داده و پردازش امن تأکید شده است (۱۰، ۳۳). از این منظر، می‌توان گفت که مدل اروپایی، پیش از توسل به حقوق کیفری، از ظرفیت ابزارهای فنی، اداری و تنظیمی برای کاهش خطر نقض حقوق اشخاص استفاده می‌کند.

در این الگو، «رضایت» نیز تنها یکی از مبانی قانونی پردازش داده‌های شخصی است و نباید آن را معادل مبنای عام

تمامی حقوق انتشار این اثر، متعلق به پژوهشکده اخلاق زیستی و حقوق سلامت پارس می‌باشد

مشروعیت پردازش دانست، زیرا مقررات عمومی اتحادیه اروپا مبانی حقوقی دیگری، از جمله انجام تعهد قانونی، حمایت از منافع حیاتی، انجام وظیفه در راستای منافع عمومی و منافع مشروع را نیز شناسایی کرده است. در مورد داده‌های سلامت، به دلیل قرارگرفتن این داده‌ها در زمره داده‌های حساس، شرایط و محدودیت‌های خاصی نیز بر پردازش آن‌ها حاکم است (۳۰). بنابراین، منطق حقوقی اروپا بیشتر بر «مشروعیت و کنترل فرایند پردازش» استوار است تا صرفاً بر «مجازات دارنده داده.»

از منظر سیاست کیفری، این ساختار را می‌توان نمونه‌ای از الگوی تنظیم‌گرای پیشگیرانه دانست که در آن حقوق کیفری، در کنار ابزارهای اداری، مدنی و فنی قرار می‌گیرد و لزوماً نخستین ابزار واکنش به نقض مقررات داده نیست، البته این امر به معنای فقدان ضمانت‌اجراهای کیفری در کشورهای عضو نیست، بلکه به این معناست که تعیین حدود و شرایط جرم‌انگاری بسیاری از رفتارهای مرتبط با داده تا حد قابل توجهی در سطح حقوق ملی دولت‌های عضو باقی می‌ماند (۳۳)، در نتیجه، از منظر تطبیقی، ویژگی مهم الگوی اروپایی را می‌توان در تقدم «حکمرانی و مدیریت خطر داده» بر «جرم‌انگاری مستقیم صرف نگهداری داده» مشاهده کرد، رویکردی که با اصل تناسب و ایده حداقل‌گرایی در مداخله کیفری سازگاری بیشتری دارد.

۱۱-۲. ایالات متحده: مسئولیت کیفری محدود در کنار اجرای اداری: در نظام حقوقی ایالات متحده نیز با وجود گستردگی مقررات مربوط به حفاظت از داده‌های سلامت، به ویژه در چارچوب استاندارد محافظت از اطلاعات شخصی و حساس بیماران، رویکرد غالب بر اجرای اداری و نظارتی استوار است و مسئولیت کیفری جایگاهی محدود دارد. در این نظام، جرم‌انگاری معمولاً زمانی فعال می‌شود که دسترسی، نگهداری یا افشای داده با قصد سوءاستفاده، انتفاع نامشروع، یا نقض آگاهانه الزامات قانونی همراه باشد؛ به همین دلیل، صرفِ در اختیارداشتن داده‌های پزشکی، بدون عنصر ذهنیِ ناظر بر سوءنیت یا بدون رفتار مترتب بر بهره‌برداری غیر مجاز، به سختی می‌تواند مبنای مسئولیت کیفری قرار گیرد.

ویژگی مهم نظام آمریکا آن است که در آن، مرز میان مسئولیت اداری، مدنی و کیفری به صورت نسبتاً دقیق ترسیم می‌شود. این تفکیک سبب می‌گردد که جرم‌انگاری صرفاً در مواردی به کار رود که نقض قواعد حفاظتی، از سطح تخلف سازمانی فراتر رفته و به سطح رفتار مجرمانه قابل سرزنش برسد. از این منظر، استاندارد محافظتی یادشده را باید نمونه‌ای از نظامی دانست که به جای جرم‌انگاری گسترده «داشتن» داده، بر نظارت، جریمه‌های اداری، مسئولیت حرفه‌ای و الزامات سازمانی تکیه دارد. همین امر سبب می‌شود که در ایالات متحده نیز، گرچه حریم خصوصی و سلامت داده از اهمیت بالایی برخوردارند، اما قانون‌گذار تمایل چندانی به جرم‌انگاری خودِ تصرف ندارد، مگر در مواردی که عنصر سوءنیت و خطر واقعی به‌روشنی احراز شود. این امر با این تحلیل هماهنگ است که در حقوق کیفری داده، باید میان «نگهداری منفعل» و «نگهداری همراه با قصد بهره‌برداری یا نقض آگاهانه» تفاوت نهاد (۳۰، ۳۷).

۱۱-۳. آلمان: دقت مفهومی، کنترل دسترسی و مسئولیت حرفه‌ای: نظام حقوقی آلمان از حیث دقت مفهومی در تعریف داده‌های حساس و نحوه تنظیم دسترسی به آن‌ها جایگاه مهمی در این مقایسه دارد. در این نظام، حفاظت از داده‌های سلامت نه فقط از طریق قواعد عام حمایت از داده، بلکه از رهگذر تأکید بر کنترل دسترسی، محدودیت هدف، مسئولیت حرفه‌ای و اصل ضرورت پیش می‌رود (۳۸)، در نتیجه، نگهداری داده سلامت در آلمان، بیش از آنکه موضوع جرم‌انگاری گسترده باشد، موضوع تنظیم‌گری دقیق و مسئولیت‌پذیری نهادی است.

وجه تمایز آلمان در این است که مفهوم داده حساس با دقت بالا صورت‌بندی می‌شود و برای هرگونه دسترسی یا پردازش، توجیه قانونی و سازمانی مشخص لازم است. این امر نشان می‌دهد که سیاست حقوقی آلمان اساساً به سمت مدیریت خطر و تفکیک سطوح دسترسی حرکت کرده است.

تمامی حقوق انتشار این اثر، متعلق به پژوهشکده اخلاق زیستی و حقوق سلامت پارس می‌باشد

از این رو، حتی اگر نگهداری داده به ظاهر به صورت فیزیکی یا فنی در اختیار یک نهاد قرار داشته باشد، این امر به تنهایی کفایت نمی‌کند، بلکه باید احراز شود که شخص یا نهاد، نسبت به داده آگاهی داشته، امکان کنترل آن را در اختیار داشته و از آن در چارچوبی ناموجه استفاده کرده است، بدین‌ترتیب، آلمان نمونه‌ای از رویکردی است که به جای جرم‌انگاری نفس تصرف، به رابطه میان دسترسی، کنترل و مسئولیت توجه می‌کند (۱۰).

از منظر سیاست کیفری، این رویکرد با اصل حداقل مداخله سازگار است، زیرا بسیاری از خطرات مرتبط با داده‌های سلامت از طریق سازوکارهای غیر کیفری قابل مهارند. در واقع، نظام آلمان نشان می‌دهد که هرچه تعریف داده حساس دقیق‌تر و معماری دسترسی شفاف‌تر باشد، نیاز به توسعه قلمرو کیفری کاهش می‌یابد، در نتیجه، جرم‌انگاری تنها در مرحله‌ای مطرح می‌شود که نقض عمدی، شدید و زیان‌بار قواعد حفاظتی محرز گردد (۳۰).

۱۱-۴. ژاپن: انضباط سازمانی و تأکید بر کنترل فنی: در ژاپن نیز گرایش غالب در حوزه داده‌های سلامت، بر تأمین امنیت، انضباط سازمانی و کنترل فنی داده متمرکز است. در این نظام، همانند آلمان، داده‌های حساس در کانون توجه قانون‌گذار قرار دارند، اما راهبرد اصلی، ایجاد چارچوبی برای صیانت از داده از طریق استانداردهای سازمانی و فنی است، نه گسترش بی‌ضابطه ضمانت‌اجراهای کیفری. این امر نشان می‌دهد که ژاپن نیز در زمره نظام‌هایی قرار می‌گیرد که به جای جرم‌انگاری گسترده نگهداری داده، به پیشگیری نهادی و کنترل دسترسی تکیه دارند (۱۰).

تحلیل سیاست کیفری ژاپن نشان می‌دهد که نگهداری داده، زمانی واجد اهمیت کیفری می‌شود که با نقض آشکار مقررات، عدم رعایت الزامات امنیتی یا سوءاستفاده از دسترسی همراه باشد. در غیر این صورت، خودِ وجود داده در یک سامانه یا نزد یک کارگزار، به تنهایی دلالت بر تحقق رفتار مجرمانه ندارد. این رویکرد به ویژه برای حقوق ایران اهمیت دارد، زیرا نشان می‌دهد که می‌توان با طراحی قواعد روشن در زمینه طبقه‌بندی داده، سطوح دسترسی، مسئولیت حرفه‌ای و الزامات امنیتی، از توسعه بی‌رویه مداخله کیفری جلوگیری کرد (۳۷).

۱۱-۵. الگوی مشترک در نظام‌های منتخب: جرم‌انگاری به عنوان آخرین ابزار: آنچه از مقایسه اتحادیه اروپا، ایالات متحده، آلمان و ژاپن به دست می‌آید، ظهور یک الگوی مشترک است: جرم‌انگاری نگهداری داده‌های حساس نه به عنوان ابزار نخست، بلکه به عنوان آخرین ابزار سیاست کیفری به کار می‌رود. در این الگو، نخست بر تنظیم‌گری اداری، کنترل فنی، الزامات سازمانی، رضایت آگاهانه، شفافیت پردازش و مسئولیت حرفه‌ای تأکید می‌شود، سپس اگر این سازوکارها ناکافی باشند و رفتار مورد نظر واجد خطر جدی، عمدی و قابل انتساب باشد، مداخله کیفری مطرح می‌شود.

این نتیجه از آن جهت اهمیت دارد که نشان می‌دهد حقوق کیفری معاصر در حوزه داده‌های سلامت، از منطق «مجازات‌محوری» به سمت منطق خطرمحوری محدود حرکت کرده است. به بیان دیگر، جرم‌انگاری تنها زمانی توجیه دارد که سه شرط هم‌زمان وجود داشته باشد: نخست، رفتار مزبور تهدیدی واقعی برای حقوق و منافع اشخاص ایجاد کند؛ دوم، این تهدید از طریق ابزارهای کم‌هزینه‌تر قابل مهار نباشد؛ سوم، میان شخص و داده رابطه‌ای از جنس آگاهی، دسترسی مؤثر و امکان کنترل برقرار باشد. در غیر این صورت، اتکای صرف به جرم‌انگاری می‌تواند به گسترش ناموجه حقوق کیفری و تضعیف اصل تناسب بینجامد (۱۰).

۱۲. مفهوم «داشتن» در فضای دیجیتال: فراتر از تصرف فیزیکی: یکی از مهم‌ترین دستاوردهای تحلیل تطبیقی این است که مفهوم تصرف در فضای دیجیتال دیگر نمی‌تواند به صورت سنتی و بر پایه تصرف فیزیکی فهم شود. در محیط داده‌محور، «داشتن» باید بر اساس سه عنصر اساسی سنجیده شود: آگاهی از وجود داده، دسترسی مؤثر به آن و امکان کنترل یا بهره‌برداری از آن. اگر این سه عنصر احراز نشود، صرف اینکه داده در یک سرور، سامانه، زیرساخت یا محیط فنی قرار دارد، برای انتساب مسئولیت کیفری کافی نیست (۱۰).

تمامی حقوق انتشار این اثر، متعلق به پژوهشکده اخلاق زیستی و حقوق سلامت پارس می‌باشد

این تحلیل از حیث نظری اهمیت زیادی دارد، زیرا نشان می‌دهد که در فضای دیجیتال، داده ممکن است در اختیار یک سامانه باشد، اما در اختیار واقعی شخص نباشد. به عبارت دیگر، وجود فنی داده با تصرف حقوقی یا کیفری یکسان نیست. بنابراین حقوق کیفری نباید صرف حضور داده در محیط اطلاعاتی را معادل «داشتن» تلقی کند. آنچه اهمیت دارد، میزان سلطه واقعی بر داده، قابلیت دسترسی و امکان بهره‌برداری است. این تفکیک از توسعه مسئولیت کیفری بر مبنای وضعیت‌های صرفاً فنی و غیر قابل کنترل جلوگیری می‌کند و به اصل شخصی‌بودن مسئولیت کیفری نیز نزدیک‌تر است (۳۷).

از سوی دیگر، این برداشت با منطق نظام‌های تطبیقی یادشده هماهنگ است، زیرا هر چهار نظام، به صورت مستقیم یا غیر مستقیم، به جای تمرکز بر حضور صرف داده، بر میزان آگاهی و کنترل تأکید دارند. به همین دلیل، مفهوم تصرف در حوزه دیجیتال باید بازتعریف شود تا بتواند در عین حفظ کارآمدی سیاست کیفری، از افراط کیفری جلوگیری کند.

۱۳. جمع‌بندی تطبیقی و دلالت‌های آن برای حقوق ایران: در مجموع، تحلیل تطبیقی نشان می‌دهد که الگوی مسلط در نظام‌های پیشرو، مبتنی بر حکمرانی داده، تنظیم‌گری پیشگیرانه، مسئولیت سازمانی و کنترل دسترسی است و نه جرم‌انگاری گسترده نگهداری داده‌های پزشکی حساس. اتحادیه اروپا بیش از همه بر تنظیم‌گری پیشینی و شفافیت پردازش تکیه دارد؛ ایالات متحده بر اجرای اداری و مسئولیت کیفری محدود؛ آلمان بر دقت مفهومی، محدودیت هدف و مسئولیت حرفه‌ای و ژاپن بر کنترل فنی و انضباط سازمانی. حاصل مشترک این نظام‌ها آن است که جرم‌انگاری، زمانی موجه است که رفتار مورد نظر با قصد یا علم همراه بوده، خطر واقعی ایجاد کند، و راه حل‌های غیر کیفری برای مهار آن ناکافی باشند.

این یافته‌ها برای حقوق ایران دارای اهمیت مستقیم است: نخست آنکه نشان می‌دهد برای مواجهه با داده‌های پزشکی حساس، ضرورتی به توسعه بی‌ضابطه قلمرو کیفری وجود ندارد؛ دوم آنکه قانون‌گذار می‌تواند با تعریف دقیق داده پزشکی حساس، تبیین روشن مفهوم «داشتن» در محیط دیجیتال، تفکیک میان نگهداری مجاز و غیر مجاز و ایجاد سازوکارهای حکمرانی داده، زمینه یک سیاست کیفری متوازن را فراهم آورد؛ سوم آنکه هرگونه جرم‌انگاری در این حوزه باید در چارچوب اصول قانونی‌بودن، تناسب، حداقل‌گرایی کیفری و ضرورت مداخله انجام شود. از همین رو، تجربه تطبیقی نه‌تنها مبنای نظری برای تحلیل مسأله فراهم می‌کند، بلکه به طور مستقیم در طراحی راه‌حل‌های تقنینی برای حقوق ایران نیز راهگشاست (۴۱-۳۹).

۱۴. چالش‌های سیاست کیفری سلامت دیجیتال در ایران: در این بخش، مهم‌ترین چالش‌های سیاست کیفری سلامت دیجیتال در ایران، خلأ و پراکندگی مقررات و دشواری تعیین و اثبات رابطه واقعی اشخاص با داده‌های پزشکی حساس است. این چالش‌ها ضرورت بازنگری در چارچوب تقنینی و تعیین دقیق حدود مسئولیت کیفری در فرایند نگهداری و کنترل داده‌های سلامت را آشکار می‌سازد.

۱۴-۱. خلأ تقنینی: نظام حقوقی ایران در حوزه سلامت دیجیتال با خلأهای تقنینی متعددی مواجه است که ناشی از سرعت پایین قانون‌گذاری در برابر تحولات تکنولوژیک می‌باشد. قانون تجارت الکترونیکی (۱۳۸۲ ش.) و قانون جرائم رایانه‌ای (۱۳۸۸ ش.) به عنوان ستون‌های اصلی، فاقد پیش‌بینی‌های اختصاصی برای چالش‌های نوظهور در سلامت دیجیتال (مانند درمان از راه دور یا پردازش داده‌های ژنتیکی) هستند. فقدان یک قانون جامع در خصوص «حفاظت از داده‌های سلامت» موجب شده است که نظارت بر سکوهای سلامت آنلاین صرفاً به بخشنامه‌های اداری محدود شود که قدرت بازدارندگی کیفری لازم را ندارند. این خلأ باعث ایجاد «ناامنی حقوقی» برای بیماران و پزشکان شده است که با اصل «قانونی‌بودن جرائم و مجازات‌ها» در تضاد است (۳۹، ۴۲).

۱۴-۲. دشواری اثبات «داشتن» در محیط دیجیتال: یکی از چالش‌های بنیادین در سیاست کیفری، اثبات تصرف یا کنترل بر داده‌های سلامت است. در جرائمی مانند «نفوذ غیر

تمامی حقوق انتشار این اثر، متعلق به پژوهشکده اخلاق زیستی و حقوق سلامت پارس می‌باشد

مجاز» یا «سرقت اطلاعات حساس پزشکی»، اثبات اینکه چه کسی کنترل داده را در اختیار داشته، به دلیل ماهیت فرار و تغییرپذیر داده‌های دیجیتال بسیار دشوار است برخلاف جرائم سنتی، در محیط دیجیتال، مفهوم «داشتن» به سادگی قابل احراز نیست، چراکه داده‌ها ممکن است در سرورهای ابری توزیع شده باشند. این پیچیدگی فنی باعث می‌شود که فرآیند کشف جرم و انتساب مسئولیت کیفری با دشواری‌های ادله‌ای مواجه شود که در نهایت منجر به افزایش نرخ «احساس ناامنی» در استفاده از خدمات سلامت دیجیتال در ایران می‌گردد (۴۳).

۱۵. نوآوری‌های پژوهش در سلامت دیجیتال: این پژوهش با هدف گذار از رویکردهای سنتی در سیاست کیفری و تطبیق آن با واقعیت‌های سلامت دیجیتال، نوآوری‌هایی را در سه محور اساسی ارائه می‌دهد:

۱۵-۱. نوآوری در تبیین مفهومی: بازتعریف مسئولیت در اکوسیستم هوشمند: در این محور، پژوهش حاضر از مدل‌های کلاسیک مسئولیت کیفری فراتر رفته و «مسئولیت الگوریتم‌محور» را در پزشکی دیجیتال معرفی می‌کند. برخلاف رویه‌های موجود که اغلب بر کنشگر انسانی متمرکز است، این پژوهش نشان می‌دهد که چگونه ابهام در کنشگری «سیستم‌های خودمختار» مرزهای مسئولیت را مخدوش کرده است. با استناد به منابع جدید (۴۴) این بخش پیشنهاد می‌دهد که برای جرائم سلامت دیجیتال، «مسئولیت مبتنی بر نظارت بر هوش مصنوعی» جایگزین مسئولیت مبتنی بر تقصیر فردی شود.

۱۵-۲. نوآوری در پیشنهاد تقنینی: تنظیم‌گری مبتنی بر ریسک: این پژوهش با نقد خلأهای تقنینی ایران، نوآوری خود را در ارائه یک «مدل تنظیم‌گری پویا» ارائه می‌دهد. برخلاف قوانین ایستا و مبتنی بر مجازات صرف، این پژوهش با الهام از مقررات پیشرو (همچون مقررات عمومی حفاظت از داده اتحادیه اروپا و پیش‌نویس‌های جدید سلامت هوشمند در اتحادیه اروپا ۲۰۲۵ م.)، گذار به سمت «تنظیم‌گری مبتنی بر ریسک» را پیشنهاد می‌کند (۳۰).

این رویکرد به جای جرم‌انگاری پسینی، بر پیشگیری ساختاری تأکید دارد. این مدل برای اولین بار به عنوان الگویی بومی برای نظام حقوقی ایران پیشنهاد شده است.

۱۵-۳. نوآوری در فرآیند اثبات: گذار از «داشتن سنتی» به «ردپای دیجیتال»: دشواری اثبات «داشتن» داده‌های پزشکی در محیط دیجیتال، یکی از چالش‌های بنیادین پژوهش است. نوآوری این بخش در معرفی مفهوم «اثبات مبتنی بر لاگ‌های دیجیتال» و استفاده از شواهد بررسی علمی ادله کشف واقعیت (Forensics) است. این مطالعه پیشنهاد می‌دهد که برای مقابله با دشواری‌های اثبات، باید ادله الکترونیکی سلامت، برخلاف ادله فیزیکی، با تکیه بر تحلیل متاداده‌ها و زنجیره بلوکی بازشناسی شوند (۴۵). این رویکرد تحول در آیین دادرسی کیفری سلامت‌محور محسوب می‌شود.

می‌توان چنین نتیجه گرفت که این سه نوآوری در کنار هم، ساختارِ پیشنهادیِ پژوهش برای «سیاست کیفری نوین سلامت دیجیتال در ایران» را تشکیل می‌دهند که همگام با استانداردهای جهانی، قابلیت اجرا و بازدارندگی در محیط پیچیده داده‌های سلامت را دارد (۴۵).

۱۶. پارادایم‌های نوین در حکمرانی داده‌های سلامت: به سوی یک نظام مسئولیت‌پذیر: در سال‌های ۲۰۲۵ و ۲۰۲۶، حکمرانی داده‌های سلامت از یک مقوله صرفاً فنی یا اداری به یک رکن بنیادین در سیاست‌گذاری حقوقی و کیفری تبدیل شده است. تحولات اخیر در اسناد بالادستی و رویه‌های نظارتی نشان می‌دهد که مفهوم سنتی «داشتن داده» در فضای دیجیتال دستخوش دگرگونی شده و اکنون با مفاهیم «کنترل مؤثر»، «قابلیت انتساب» و «مسئولیت‌پذیری در زنجیره تأمین داده» گره خورده است. این تغییر پارادایم، به ویژه در واکنش به افزایش بی‌سابقه حملات سایبری علیه زیرساخت‌های بهداشتی، ضرورت بازتعریف مسئولیت کیفری نگهدارندگان داده را به یک اولویت تبدیل کرده است (۳۳، ۳۶).

تمامی حقوق انتشار این اثر، متعلق به پژوهشکده اخلاق زیستی و حقوق سلامت پارس می‌باشد

بر اساس تحلیل‌های منتشرشده در سال ۲۰۲۶، تمرکز نهادهای ناظر از نظارتِ انفعالی بر محرمانگی داده‌ها به سمت «حکمرانی جامع و پیش‌دستانه» حرکت کرده است. در ایالات متحده، وزارت بهداشت و خدمات انسانی با پیشنهاد اصلاحات اساسی در نظام استاندارد حفظ حریم خصوصی در آغاز سال ۲۰۲۵، استانداردهای سخت‌گیرانه‌تری را برای نهادهای پوشش‌دهنده و پیمانکاران مرتبط وضع نموده است. این مقررات جدید، «مدیریت ریسک سایبری» را نه یک انتخاب، بلکه یک تکلیف قانونیِ مبتنی بر الزامات فنی دقیق (مانند احراز هویت چند عاملی، رمزنگاری و پایش مستمر) می‌داند (۳۴). از منظر سیاست کیفری، این بدان‌معناست که صرفِ «داشتنِ داده» بدون استقرار این تدابیر ایمنی، می‌تواند به عنوان «قصور در صیانت» و زمینه‌ساز مسئولیت کیفری قلمداد شود (۳۷).

علاوه بر این، روندهای گزارش‌شده در سال ۲۰۲۶ نشان می‌دهند که با پیچیده‌ترشدن جریان داده‌ها و ورود هوش مصنوعی به فرآیندهای بالینی، «زنجیره تأمین داده» به کانون آسیب‌پذیری تبدیل شده است. گزارش‌های تحلیلی اخیر تأکید دارند که نهادهای درمانی اکنون مسئولیت سنگین‌تری در قبال نظارت بر اشخاص ثالث دارند. این توسعه‌یافتگیِ مسئولیت، پاسخگوی چالش‌های نوظهوری است که در آن نشت داده نه‌تنها ناشی از یک نفوذ مستقیم، بلکه نتیجه بی‌توجهی به پروتکل‌های امنیتی در سطحِ دسترسی‌های ثالث است (۵)، لذا در نظام حقوقیِ مدرن، «داشتن داده» با «تعهد به حفاظت فعال» هم‌معنا شده است.

از سوی دیگر، تحولات اخیر در اتحادیه اروپا و سایر حوزه‌های قضایی پیشرو در سال ۲۰۲۶، بر مفهوم «حداقل‌گرایی داده» تأکید مضاعف دارند. مطابق با آخرین تحلیل‌های مربوط به اجرای چارچوب‌های جدید حریم خصوصی، نگهدارنده داده موظف است نه‌تنها از داده محافظت کند، بلکه باید چرخه حیات داده را به گونه‌ای مدیریت کند که کمترین ریسک برای حریم خصوصی بیمار ایجاد شود (۳۳). این رویکرد، پاسخی است به چالش‌های حکمرانی در عصری که حجم داده‌های تولیدشده در نظام سلامت به صورت نمایی در حال افزایش است.

برای سیاست‌گذار ایرانی، این تحولات ۲۶-۲۰۲۵ واجد دو پیام راهبردی است: نخست، ضرورت عبور از نگاه سنتی به «داشتن داده» و پذیرش مدل «مسئولیت مبتنی بر ریسک»؛ دوم، لزوم تدوین مقرراتی که در آن جرم‌انگاری، به جای تمرکز بر نفسِ نگهداری داده، بر «قصور در استقرار تدابیر امنیتی» و «ایجاد ریسک غیر منطقی» متمرکز باشد. چنانچه در نظام حقوقی ایران، تعریفی از «داده حساس پزشکی» ارائه شود که با استانداردهای امنیتی ۲۰۲۶ همخوانی داشته باشد، می‌توان انتظار داشت که سیاست کیفریِ سلامت دیجیتال از یک نظامِ مبهم به نظامی پیش‌بینی‌پذیر، بازدارنده و متناسب با تحولات فناوری نوین تبدیل گردد (۴۱).

در نهایت، همگرایی اسناد بین‌المللی در سال ۲۰۲۶ نشان می‌دهد که امنیت سایبری در نظام سلامت، دیگر نه یک موضوع فنی، بلکه یک «حق بشریِ نوظهور» است که دولت‌ها در چارچوب سیاست‌های کیفری خود ملزم به صیانت از آن هستند (۳۷). بنابراین، پیشنهادات تقنینی برای ایران باید با نگاه به این افقِ جهانی و با تکیه بر «امنیت از طریق طراحی (Security by Design)» تنظیم گردد تا از بروز خلأهای قانونی در مواجهه با چالش‌های دیجیتال پیش رو مصون بماند.

روش

این پژوهش با روش توصیفی ـ تحلیلی و رویکرد تطبیقی انجام شده است. داده‌های پژوهش از طریق مطالعه اسناد و منابع کتابخانه‌ای، قوانین و مقررات مرتبط، آرای قضایی و ادبیات حقوقی کشورهای منتخب گردآوری و با استفاده از روش تحلیل حقوقی و تطبیقی بررسی شده‌اند. در این فرایند، مبانی جرم‌انگاری نگهداری و داشتن غیر مجاز داده‌های پزشکی با تأکید بر اصول قانونی بودن جرم و مجازات، اصل ضرر، اصل تناسب و الزامات حمایت از حریم خصوصی و امنیت اطلاعات ارزیابی شده است.

تمامی حقوق انتشار این اثر، متعلق به پژوهشکده اخلاق زیستی و حقوق سلامت پارس می‌باشد

ملاحظات اخلاقی

در پژوهش حاضر جنبه‌های اخلاقی مطالعه کتابخانه‌ای شامل اصالت متون، صداقت و امانتداری رعایت شده است.

یافته‌ها

یافته‌های پژوهش نشان می‌دهد که در برخی نظام‌های حقوقی پیشرو، رویکرد کیفری نسبت به داده‌های پزشکی از تمرکز صرف بر «افشای بالفعل داده» به سمت شناسایی و کنترل «خطر بالقوه ناشی از نگهداری غیر مجاز داده» در حال تحول است. بر این اساس، داشتن داده‌های پزشکی حساس، در صورتی که بدون مجوز قانونی یا برخلاف الزامات امنیتی صورت گیرد و قابلیت ایجاد خطر معنادار برای حریم خصوصی، امنیت اطلاعات یا اعتماد درمانی را داشته باشد، می‌تواند واجد وصف کیفری شود. با این حال، یافته‌ها نشان می‌دهد که جرم‌انگاری صرفِ وضعیت داشتن داده، بدون احراز شرایطی همچون غیر مجاز بودن، قابلیت انتساب و وجود خطر معنادار، با اصول بنیادین حقوق کیفری، به ویژه اصل قانونی‌بودن، اصل ضرر و اصل تناسب، سازگار نیست. از این رو، تفکیک میان نگهداری حرفه‌ای و مشروع داده‌های پزشکی و نگهداری غیر مجاز و خطرزای آن، شرط اساسی مشروعیت مداخله کیفری است.

بحث

گسترش حکمرانی دیجیتال در حوزه سلامت، موجب تولید و انباشت حجم گسترده‌ای از داده‌های پزشکی حساس شده است؛ داده‌هایی که صرفِ دسترسی، نگهداری یا در اختیار داشتن غیر مجاز آن‌ها می‌تواند زمینه‌ساز نقض حریم خصوصی و ورود آسیب‌های جدی به حقوق و آزادی‌های فردی باشد. از این منظر، مسأله اساسی آن است که آیا «داشتن» داده‌های پزشکی حساس، مستقل از افشا یا استفاده زیان‌بار از آن‌ها، می‌تواند واجد چنان وصف مجرمانه‌ای باشد که مداخله حقوق کیفری را توجیه کند. پاسخ به این پرسش مستلزم بررسی مبانی جرم‌انگاری، اصول حاکم بر سیاست کیفری، حدود مسئولیت اشخاص و نهادهای متولی داده و نیز چالش‌های ناشی از تحول فناوری‌های دیجیتال در نظام سلامت است.

نتیجه‌گیری

پژوهش حاضر با بررسی ابعاد مختلف سلامت دیجیتال در پرتو سیاست کیفری، نشان داد که پارادایم کنونی نظام قضایی ایران در مواجهه با مخاطرات حوزه سلامت دیجیتال ـ از جمله نقض حریم خصوصی، خطاهای هوش مصنوعی و جرائم سایبری ـ پزشکی ـ با خلأهای تقنینی و اجرایی جدی رو به روست. تحلیل‌های تطبیقی صورت‌گرفته با نظام‌های پیشرو، مؤید آن است که اتکا به قوانین سنتی بدون در نظرگرفتن ماهیت پویای «داده‌های سلامت» نمی‌تواند امنیت حقوقی لازم را برای ذی‌نفعان فراهم کند.

بررسی مسئولیت کیفری ناشی از «داشتن داده‌های پزشکی حساس» نشان می‌دهد که توسعه سلامت دیجیتال، مرزهای سنتی جرم‌انگاری را با چالش جدی مواجه کرده است. داده‌های پزشکی به دلیل ارتباط مستقیم با کرامت انسانی، حریم خصوصی و امکان سوءاستفاده‌های گسترده، از حساس‌ترین انواع داده‌های شخصی محسوب می‌شوند؛ با این حال، صرف «در اختیارداشتن» این داده‌ها بدون تحقق رفتارهای مجرمانه تکمیلی، مانند افشا، فروش یا دسترسی غیر مجاز، از منظر اصول بنیادین حقوق کیفری ـ به ویژه اصل حداقل‌بودن مداخله کیفری و اصل تناسب ـ به سختی قابل توجیه است.

در واقع، جرم‌انگاری صرف نگهداری داده‌های پزشکی حساس می‌تواند به تورم کیفری و گسترش مسئولیت کیفری به حوزه‌های غیر مجاز منجر شود، به ویژه در محیط‌های درمانی و فناورانه که گردش داده‌ها امری اجتناب‌ناپذیر و ساختاری است. چنین رویکردی نه‌تنها کارکرد پیشگیرانه مؤثری ندارد، بلکه ممکن است موجب اختلال در تبادل اطلاعات پزشکی، کاهش اعتماد میان بازیگران نظام سلامت و حتی کندی نوآوری در حوزه سلامت دیجیتال گردد.

تمامی حقوق انتشار این اثر، متعلق به پژوهشکده اخلاق زیستی و حقوق سلامت پارس می‌باشد

از سوی دیگر، نمی‌توان نسبت به خطرات واقعی ناشی از نگهداری غیر مجاز یا ناامن داده‌های پزشکی بی‌تفاوت بود. بنابراین سیاست کیفری مطلوب باید میان «نگهداری مشروع» و «نگهداری غیر مجاز همراه با سوءنیت یا نقض امنیت داده» تفکیک قائل شود. در این چارچوب، تمرکز نظام حقوق کیفری باید بر رفتارهای دارای خطر بالفعل یا بالقوه جدی مانند دسترسی غیر مجاز، افشای اطلاعات، تجارت داده‌های سلامت و سوءاستفاده هدفمند از آن‌ها قرار گیرد، نه صرف در اختیار داشتن داده.

در نهایت، می‌توان نتیجه گرفت که سیاست کیفری کارآمد در حوزه سلامت دیجیتال باید از رویکرد جرم‌انگاری حداقلی و هدفمند پیروی کند، به گونه‌ای که ضمن حمایت مؤثر از حریم خصوصی بیماران و تضمین امنیت داده‌های پزشکی، مانع از گسترش بی‌رویه مسئولیت کیفری و اختلال در جریان مشروع داده‌های سلامت نشود. تحقق این توازن، مستلزم هماهنگی میان حقوق کیفری، مقررات حفاظت از داده و استانداردهای امنیت سایبری است.

پیشنهادات تقنینی: به منظور گذار از سیاست کیفری واکنشی به سیاست کیفری پیش‌دستانه، پیشنهادات زیر ارائه می‌گردد:

۱ـ تدوین قانون جامع سلامت دیجیتال: تصویب قانونی اختصاصی که فراتر از قوانین عام جرائم رایانه‌ای، مسئولیت‌های مدنی و کیفری پلتفرم‌های سلامت را تعریف کند؛ این قانون می‌تواند با بهره‌گیری از الگوهای حکمرانی داده در اتحادیه اروپا و تجربه مقررات عمومی حفاظت از داده اتحادیه اروپا تنظیم شود.

۲ـ تعیین تکلیف مسئولیت کیفری هوش مصنوعی: ایجاد ضوابطی که مسئولیت ناشی از خطای الگوریتم‌های تشخیصی را میان «توسعه‌دهنده»، «پزشک» و «نهاد نظارتی» تسهیم نماید.

۳ـ تغییر رویکرد در فرآیند اثبات: پذیرش ادله الکترونیک مبتنی بر بلاک‌چین برای تأیید اصالت داده‌های سلامت و تغییر بار اثبات در پرونده‌های قصور پزشکی دیجیتال به نفع بیمار.

پیشنهادات اجرایی و کاربردی: همچنین پیشنهاد الگوی اجرایی و کاربردی به ترتیب ذیل ارائه می‌گردد:

۱ـ ایجاد «صندوق بیمه مسئولیت سلامت دیجیتال»: برای پوشش خسارات ناشی از نقص‌های فنی غیر قابل پیش‌بینی که مستقیماً به کاربر وارد می‌شود.

۲ـ نظارت الگوریتمی: نهادهای نظارتی مانند وزارت بهداشت و پلیس فتا باید بازرسی دوره‌ای از کدهای برنامه‌نویسی و امنیت داده‌های پلتفرم‌های سلامت را به عنوان یک الزام قانونی در دستور کار قرار دهند.

۳ـ آموزش قضات تخصصی: تشکیل شعب ویژه رسیدگی به جرائم سلامت دیجیتال که با دانش پایه در حوزه فناوری اطلاعات آشنایی داشته باشند.

این پیشنهادات در صورتی که در کنار یک سیاست‌گذاری تعاملی ـ با مشارکت متخصصان حقوق، فناوری و پزشکی ـ اجرایی شوند، می‌توانند بستری امن برای توسعه فناوری‌های نوین در نظام سلامت کشور فراهم آورند.

مشارکت نویسندگان

زهره نیک‌فرجام: ارائه طرح، نظارت و راهنمایی بر نگارش و جمع‌بندی نهایی.

سیدمحمد کیکاوسی: جمع‌آوری داده‌ها و نگارش مقاله.

نویسندگان نسخه نهایی را مطالعه و تأیید نموده و مسئولیت پاسخگویی در قبال پژوهش را پذیرفته‌اند.

تشکر و قدردانی

ابراز نشده است.

تضاد منافع

نویسندگان هیچ‌گونه تضاد منافع احتمالی را در رابطه با تحقیق، تألیف و انتشار این مقاله اعلام نکرده‌اند.

تمامی حقوق انتشار این اثر، متعلق به پژوهشکده اخلاق زیستی و حقوق سلامت پارس می‌باشد

تأمین مالی

نویسندگان اظهار می‌نمایند که هیچ‌گونه حمایت مالی برای تحقیق، تألیف و انتشار این مقاله دریافت نکرده‌اند.

بیانیه هوش مصنوعی

در نگارش پژوهش، از هوش مصنوعی استفاده نشده است.

تمامی حقوق انتشار این اثر، متعلق به پژوهشکده اخلاق زیستی و حقوق سلامت پارس می‌باشد

References

1. Gkoulalas-Divanis A, Loukides G. Medical Data Privacy Handbook. Cham: Springer International Publishing; 2015.

2. World Health Organization. Global strategy on digital health. Geneva: World Health Organization Press; 2021.

3. Dove ES. Health Privacy Law. Cheltenham: Edward Elgar Publishing; 2026.

4. Robichau BP. Healthcare Information Privacy and Security: Regulatory Compliance and Data Security in the Age of Electronic Health Records. Berkeley: Apress; 2014.

5. Organisation for Economic Co-operation and Development. Health at a Glance 2025: OECD Indicators. Paris: OECD Publishing; 2025.

6. Greenbaum D. Cyberbiosecurity: A New Field to Deal with Emerging Threats. Cham: Springer Springer International Publishing; 2024.

7. Dove ES. Confidentiality, Privacy, and Data Protection in Biomedicine: International Concepts and Issues. London: Routledge; 2024.

8. Hutchings E, Loomes M, Butow P, Boyle FM. A systematic literature review of health consumer attitudes towards secondary use and sharing of health administrative and clinical trial data: A focus on privacy, trust, and transparency. Syst Rev. 2020; 9(1): 1-41.

9. Kim L. Healthcare Cybersecurity, Privacy, and Data Protection: Present and Future. London: Productivity Press; 2026.

10. Ashworth A, Zedner L, Tomlin P. Prevention and the Limits of the Criminal Law. Oxford: Oxford University Press; 2013.

11. Sullivan JM, Hartsfield SB. HIPAA: A Practical Guide to the Privacy and Security of Health Data. Chicago: American Bar Association, Health Law Section; 2020.

12. Hoffman S. Electronic Health Records and Medical Big Data: Law and Policy. Cambridge: Cambridge University Press; 2016.

13. Aasen H, Toebes B, Hartlev M, Hendriks A, Ó Cathaoir K, Herrmann JR. Health and Human Rights: Global and European Perspectives. 2nd ed. Cambridge: Intersentia; 2022.

14. Tzanou M. Health Data Privacy under the GDPR: Big Data Challenges and Regulatory Responses. Abingdon: Routledge; 2020.

15. Harman LB, Cornelius LJ. Ethical Health Informatics: Challenges and Opportunities. Burlington: Jones & Bartlett Learning; 2017.

16. McMahon A, Buyx A, Prainsack B. Big Data Governance Needs More Collective Responsibility: The Role of Harm Mitigation in the Governance of Data Use in Medicine and Beyond. Med Law Rev. 2020; 28(1): 155-182.

17. Nory Yoshanloey J, Azadbakht S. Legislative developments of the confidentiality principle of medical information in Iranian and French law. Iran J Med Ethics Hist Med. 2022; 15(1): 224-238. [Persian]

18. Hoffman S, Herveg J. Privacy and integrity of medical information. Edited by Orentlicher D, Hervey TK. In: The Oxford Handbook of Comparative Health Law. Oxford: Oxford University Press; 2021.

19. Organisation for Economic Co-operation and Development. Health Data Governance: Privacy, Monitoring and Research. Paris: OECD Publishing; 2015.

20. Institute of Medicine. Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. Washington: National Academies Press; 2009.

21. Gostin LO. Public Health Law: Power, Duty, Restraint. Oakland: University of California Press; 2025.

22. Tovino SA. Laws of Medicine: Core Legal Aspects for the Healthcare Professional. Cham: Springer; 2022.

23. Hordern V. The Patient, Data Protection and Changing Healthcare Models. Cambridge: Cambridge University Press; 2022.

24. Schroeder D, Gefenas E. Ethics and Law in Biobanking: Principles, Practices, and Policies. Cham: Springer; 2020.

25. Shams A. Medical Law. Tehran: Mizan Publications; 2016. [Persian]

26. Najafi Tavana A. Criminal Medical Law. Tehran: Mizan Publications; 2014. [Persian]

27. Rayejian Asli M. Information Technology Criminal Law. Tehran: Samt Publications; 2014. [Persian]

28. Mohseni F. Information Privacy: A Criminal Study in Iranian Law, United States Law and Imamiyyah Jurisprudence. Tehran: Imam Sadeq University Press; 2011. [Persian]

29. Messinis S, Temenos N, Protonotarios NE, Rallis I, Kalogeras D, Doulamis N. Enhancing Internet of

تمامی حقوق انتشار این اثر، متعلق به پژوهشکده اخلاق زیستی و حقوق سلامت پارس می‌باشد.

Medical Things security with artificial intelligence. London: Esmit Press; 2024.

30. Gellert R. The Risk-Based Approach to Data Protection. Oxford: Oxford University Press; 2020.

31. Slokenberga S, Ó Cathaoir K, Shabani M. The European Health Data Space: Examining a New Era in Data Protection. London: Routledge; 2025.

32. Sturgess J. A Medic's Guide to Essential Legal Matters. Oxford: Oxford University Press; 2018.

33. Schneider G. Health Data Pools under European Data Protection and Competition Law: Health as a Digital Business. Cham: Springer; 2022.

34. U.S. Department of Health and Human Services. Summary of the HIPAA Privacy Rule. Washington: U.S. Department of Health and Human Services; 2025.

35. Personal Information Protection Commission, Japan. Guidelines on the Act on the Protection of Personal Information: General Rules. Tokyo: Personal Information Protection Commission; 2024.

36. Federal Ministry of Health. Health Data Utilisation Act (Gesundheitsdatennutzungsgesetz - GDNG). Berlin: Federal Ministry of Health; 2024.

37. Simester AP. Fundamentals of Criminal Law: Responsibility, Culpability, and Wrongdoing. Oxford: Oxford University Press; 2021.

38. Federal Commissioner for Data Protection and Freedom of Information. Activity Report for 2024. Bonn: BfDI; 2025.

39. Ardebili MA. Public Criminal Law. Tehran: Mizan Publications; 2025. Vol.1. [Persian]

40. Zeraat A. Public Criminal Law. Tehran: Jangal Javidaneh Publications; 2021. Vols.1-2. [Persian]

41. Gorji-Azandariani A. Fundamentals of Public Law. Tehran: Jangal Javidaneh Publications; 2024. [Persian]

42. Mir-Mohammadsadeghi H. Special criminal law: Crimes against the moral personality of persons. Tehran: Mizan Publications; 2023. [Persian]

43. Jalalian A, Abbasi V. Electronic evidence in Iranian law. 2nd ed. Tehran: Dadgostar Publications; 2022. [Persian]

44. Grote T, Berens P. On the ethics of deep learning in healthcare. J Med Ethics. 2020; 46(6): 388-393.

45. Shavers B. Placing the Suspect behind the Keyboard: Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects. Burlington: Syngress; 2013.

تمامی حقوق انتشار این اثر، متعلق به پژوهشکده اخلاق زیستی و حقوق سلامت پارس می‌باشد